Responding to the Latest DNS Threats

SUMIT08

University of Michigan

21st Oct 2008

Keith Mitchell

Director of Engineering

Internet Systems Consortium

Presentation Overview

- Introduction
- Kaminsky's CERT VU#800113
- Disclosure and Mitigation
- Measuring Vulnerability
- The Case for DNSSEC

Introduction

What is the DNS ?

- Internet Domain Name System
- Provides conversion from human/application-friendly "domain names" (e.g. www.isc.org)..
- ..to network-friendly Internet Protocol addresses (e.g. 204.152.190.196, fe80::200:1aff:fe1a:2761)
- Highly distributed servers, hierarchy delegated from
  - 13 "root" servers
  - "top-level" (e.g. ".uk", ".org") servers
  - providers
  - users

What is ISC ?

- Internet Systems Consortium, Inc.
  - Headquartered in Redwood City, California
  - 501(c)(3) Nonprofit Corporation
- Mission:
  - To develop and maintain production quality Open Source software, such as BIND and DHCP
  - Enhance the stability of the global DNS through reliable F-root nameserver operations and ongoing operation of OARC
  - Further protocol development efforts, particularly in the areas of DNS evolution and facilitating the transition to IPv6.

Speaker's Background

- Internet operations and development since 1986
- Network security *survivor* rather than expert...
  - Founder and CTO of UK's first commercial ISP, *PIPEX* 1992-1996
  - Founder and Executive Chairman of London Internet Exchange, *LINX* 1994-2000
  - Founder and Director of *Nominet UK* 1996-2002
  - Chair of *RIPE NCC* Executive Board 1998-2000
  - Founder and CTO of pan-European commercial IXP operator, *XchangePoint* 2000-2004
  - Chair of *UK Network Operators' Forum* 2005-
- Moved to US (Cleveland OH) 2006-

Acknowledgements

- I am none of a researcher, security expert, nor programmer – this talk draws extensively on the hard work of others, in particular:
  - Duane Wessels, DNS-OARC
  - Sid Faber, CERT
  - Alan Clegg, ISC

CERT VU#800113

The “Kaminsky” Attack

Cache Poisoning

- The ability to introduce incorrect information into a DNS server's cache
- This information is then provided to clients

CERT VU#800113

- Dan Kaminsky discovered a new vector for an attack against DNS transactions
- Issue (small size of transaction ID) known for years, but Dan's attack vector is “more impressive”
  - exploits caching of additional RRs from spoofed responses

CERT VU#800113

- Flaw is “FedEx Logo Arrow” type of vulnerability

- Once you see it, you won't be able to “not see it”

CERT VU#800113

- Multiple DNS implementations are extremely vulnerable to this cache poisoning
- Vulnerable:
  - BIND, Cisco, Juniper, Microsoft and derivatives
- Not immediately vulnerable:
  - djbdns, powerDNS, unbound

CERT VU#800113

- Dan contacted several vendors upon discovery of the vulnerability (Feb)
- Summit held during March
  - ✓ restricted detailed disclosure
  - ✓ agreed solution and public disclosure time-line
- Plan was to have fixes ready before public announcement

Disclosure and Mitigation

Mitigation

- ISC, Cisco, Microsoft, Debian and others (but not everyone) were alerted and released code simultaneously on 8th July
- Yes, it was a Patch Tuesday
- This was a major effort

  (that is a major understatement)

The Exploit is Real

- Details of vulnerability leaked before embargo date due to blog "accident" on 21st July
- Exploit tools available within days
- Actual attacks before start August
- Official details were released to the public at Black Hat on August 7th

Source-Port Randomization

- The only long-term fix is DNSSEC
- The temporary work-around is to add randomness to each query
- Randomness is introduced in the query port number

Mitigation **not** Cure-all

- Note that even "not immediately" vulnerable servers listed earlier are still theoretically vulnerable
- The current "fix" of port randomization is remediation until DNSSEC is deployed

Mitigation **not** Cure-all

- Deploying DNSSEC is not realistic in the short term
- Port randomization of queries adds randomness, but is a temporary fix
- Update & Configure ASAP

ISC BIND Mitigation

- Install 9.3.5-P2, 9.4.2-P2, 9.5.0-P2
  - Note that initial -P1 releases **are** secure, but had possible performance and stability issues on some platforms (e.g. Solaris) which -P2 releases mitigate
  - -P1 fine if you are not seeing problems
  - -P2W2 releases address some Windows-specific issues
- Remove restrictions on query ports

```
query-source address 192.168.2.3 port 53;
```

PATs, NATs, Firewalls

- Even if you have patched your server, in some environments, CPE-edge boxes may de-randomize DNS UDP source ports
- Major enterprise vendors are aware of this and supplying patches
- Consumer broadband boxes less easy to address ☹

Other Interim fixes

- There are other ways of adding randomness as interim mitigation
- Various options being considered by IETF DNSEXT WG
- Also discussion on <dns-operations@lists.dns-oarc.net> (open) mailing list

Other Interim Fixes

- "DNS 0x20": adds unused "case" bit in query strings to increase query ID space
- Round Trip-Time Banding
- Multiple server source IP addresses
  - particularly effective for IPv6
- TCP fall-back
  - but vulnerable to denial-of-service

Measuring Vulnerability

Are you vulnerable?

- Dan Kaminsky
  - Web based interface - `www.doxpara.com`

```
Your name server, at 66.57.17.110, appears to be safe.
Requests seen for fbdfd8f7dc64.toorrr.com:
66.57.17.110:57889 TXID=65162
66.57.17.110:60521 TXID=53424
66.57.17.110:21698 TXID=32752
66.57.17.110:24178 TXID=49020
66.57.17.110:47197 TXID=25844
```

Are you vulnerable?

- Michael C. Toren
  <mct@toren.net>

- Perl based reverse engineering of Dan's javascript

  http://michael.toren.net/code/noclicky/

What is DNS-OARC ?

- Domain Name System Operations, Analysis and Research Center
- Co-ordination centre to protect Global DNS infrastructure
- Trusted, neutral environment for operators and researchers to:
  - gather and share data
  - co-ordinate response to attacks
- Holds open meetings twice a year

What is DNS-OARC ?

- Established 2004 by ISC, I served as Programme Manager from 2006-2008
  - Duane Wessels new Programme Manager
  - I am now President of OARC Inc. entity
- Now independent nonprofit membership organisation of DNS operators
- Has been gathering data on this vulnerability, analysis performed by various researchers on this data at recent OARC meeting in Ottowa in Sep

OARC Vulnerability Detectors

- `dig +short porttest.dns-oarc.net TXT`

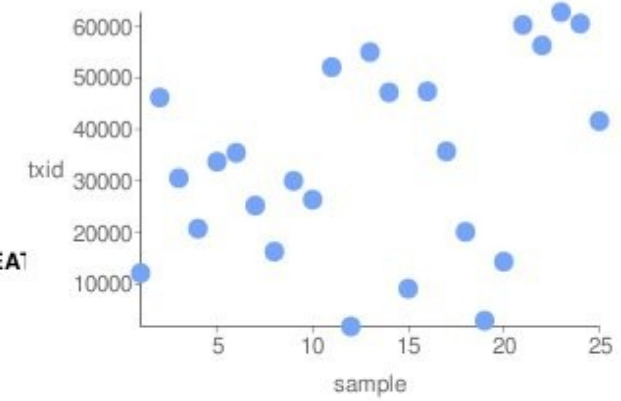
```
"66.57.17.110 is GOOD: 26 queries in 2.6
  seconds from 26 ports with std dev
  19167.29"
```

- Web-based:

  https://www.dns-oarc.net/oarc/services/dnsentropy

OARC Web Query ID Tester

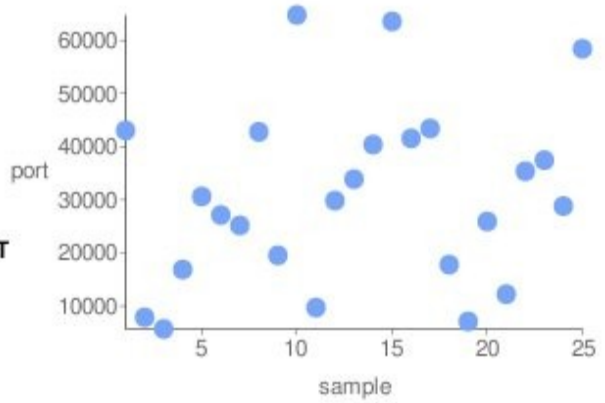
66.57.17.110 Transaction ID Randomness: GREAT



Number of samples: 25
Unique txids: 25
Range: 1747 - 62732
Modified Standard Deviation: 18690
Bits of Randomness: 16
Values Seen: 12097 46163 30527 20723 33718 35451 25210 16277 29988 26355 52063 1747 54978 47159 9086 47348 35725 20113 2878 14319 60249 56271 62732 60512 41599

OARC Web Port Tester

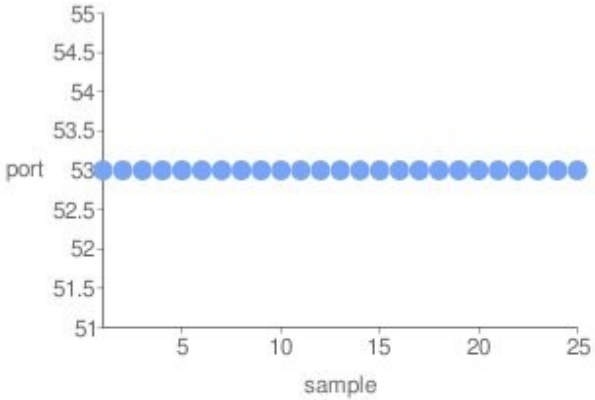
66.57.17.110 Source Port Randomness: GREAT



Number of samples: 25
Unique ports: 25
Range: 5691 - 64785
Modified Standard Deviation: 16827
Bits of Randomness: 16
Values Seen: 43054 7891 5691 16897 30628 27141 25182 42783 19549
64785 9724 29847 33894 40400 63576 41563 43425 17799
7114 25924 12237 35382 37464 28826 58425

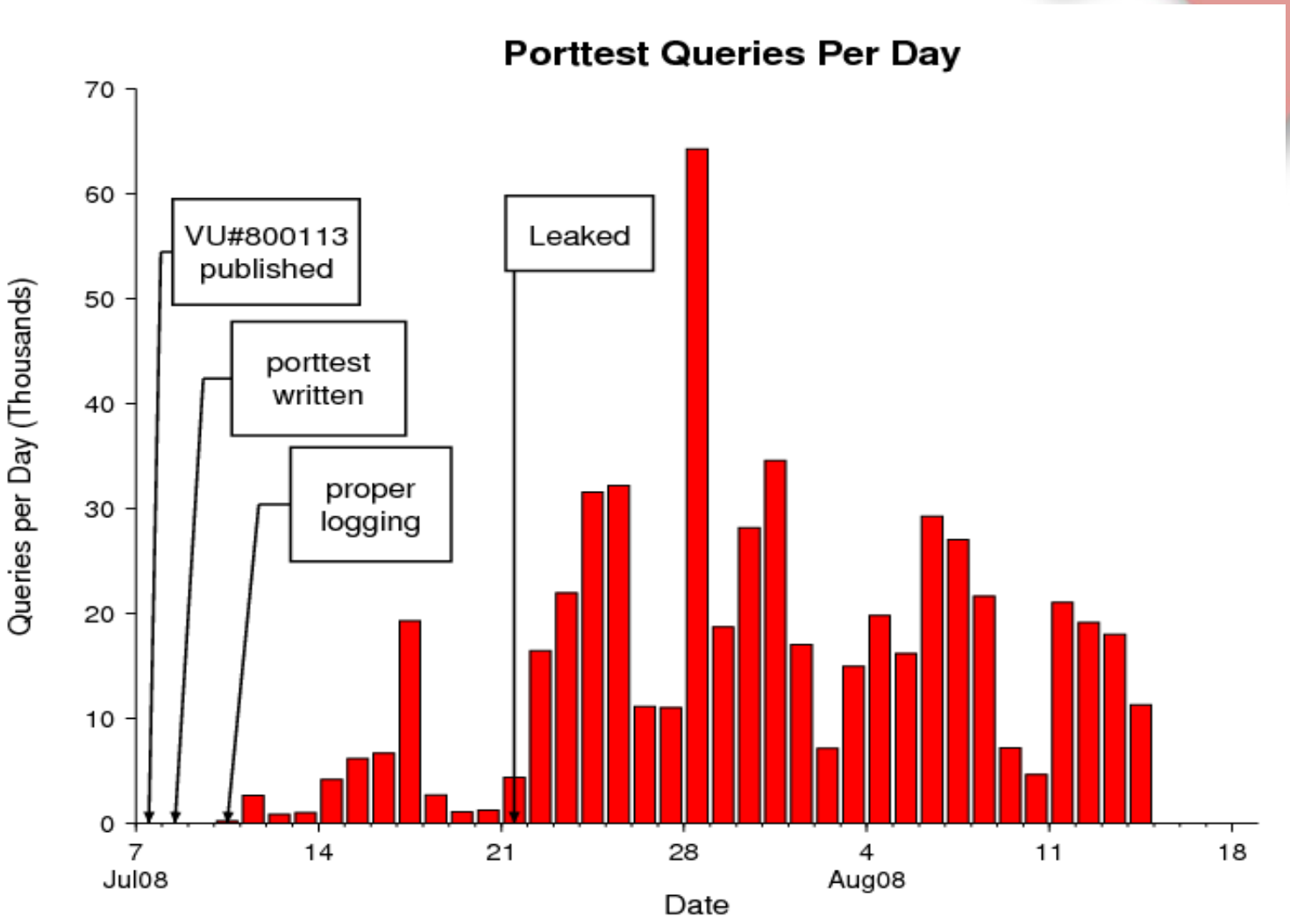
OARC Web Port Tester

207.217.126.41 Source Port Randomness: POOR

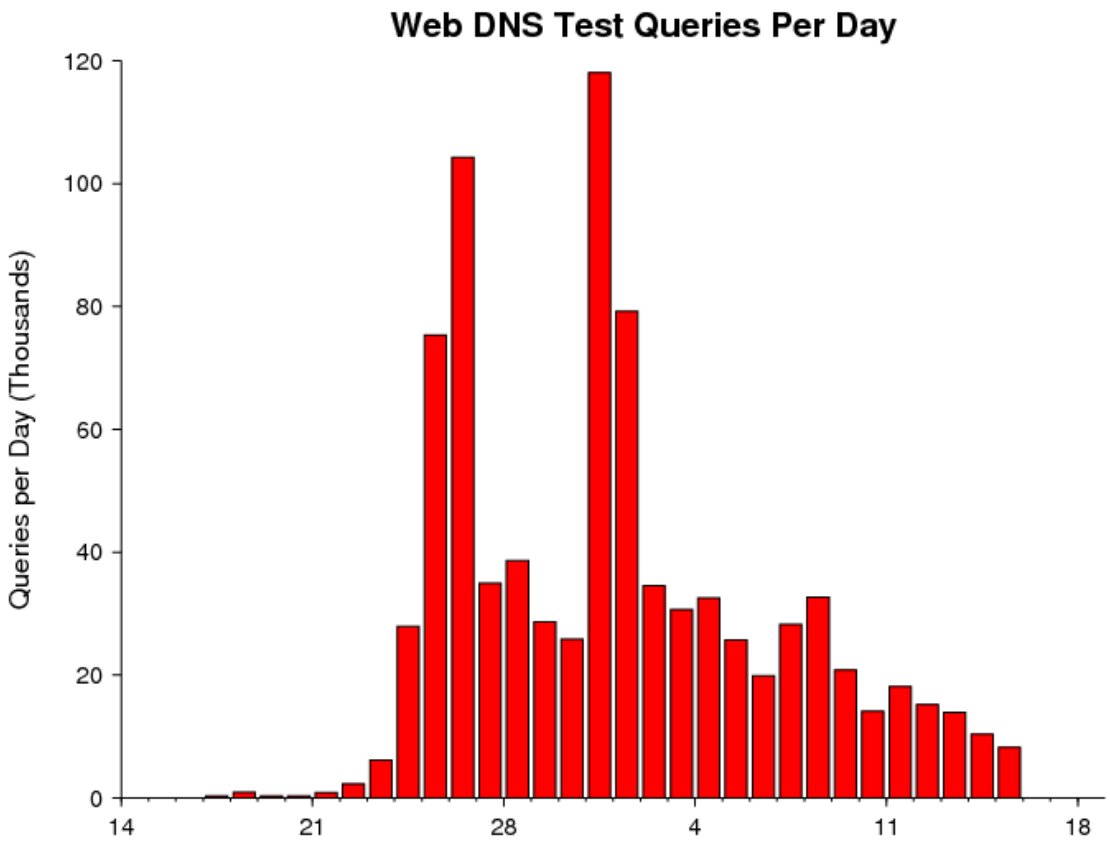


Number of samples: 25
Unique ports: 1
Range: 53 - 53
Modified Standard Deviation: 0
Bits of Randomness: 0
Values Seen: 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53

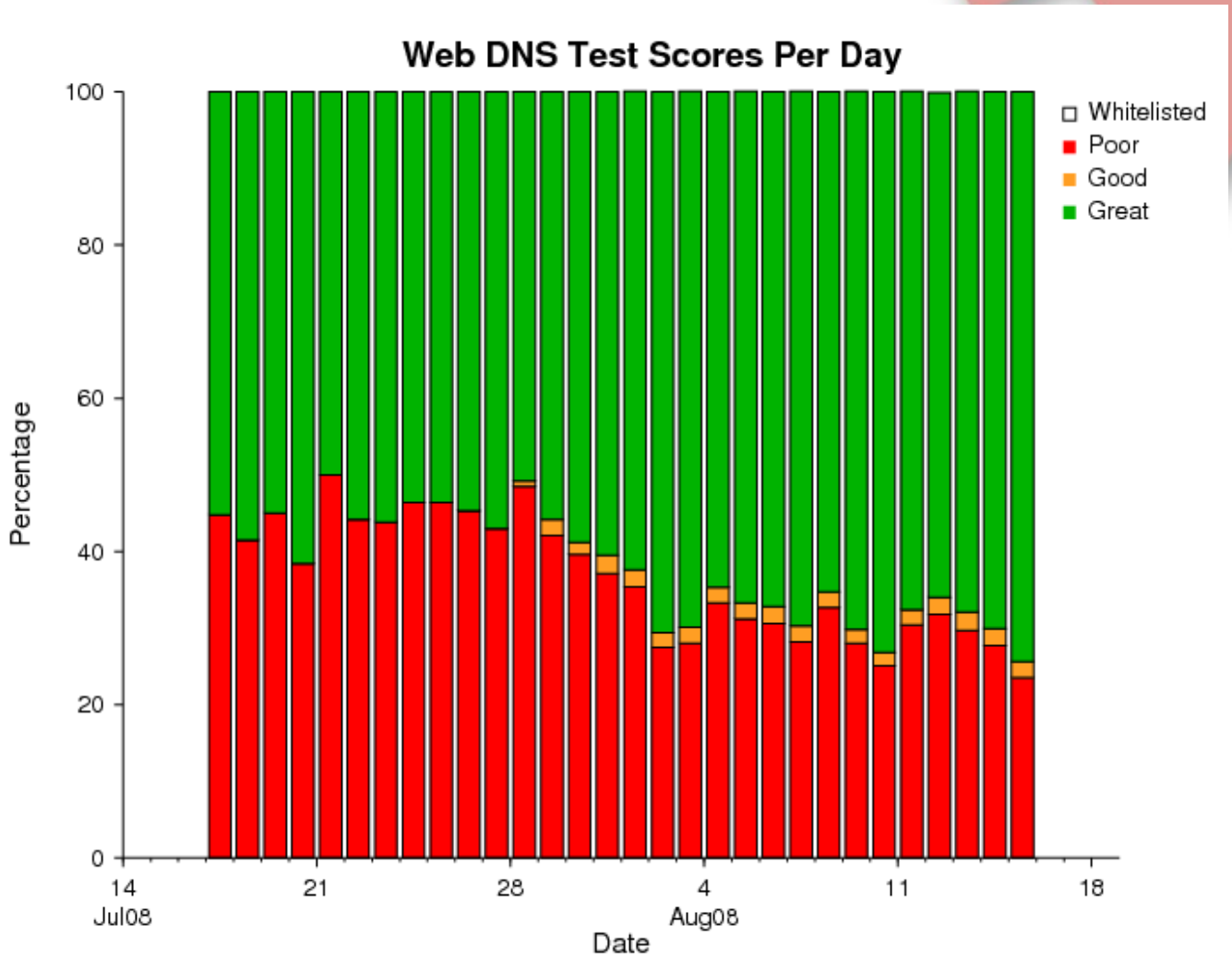
Data from OARC Port Test Tools



Data from OARC Port Test Tools



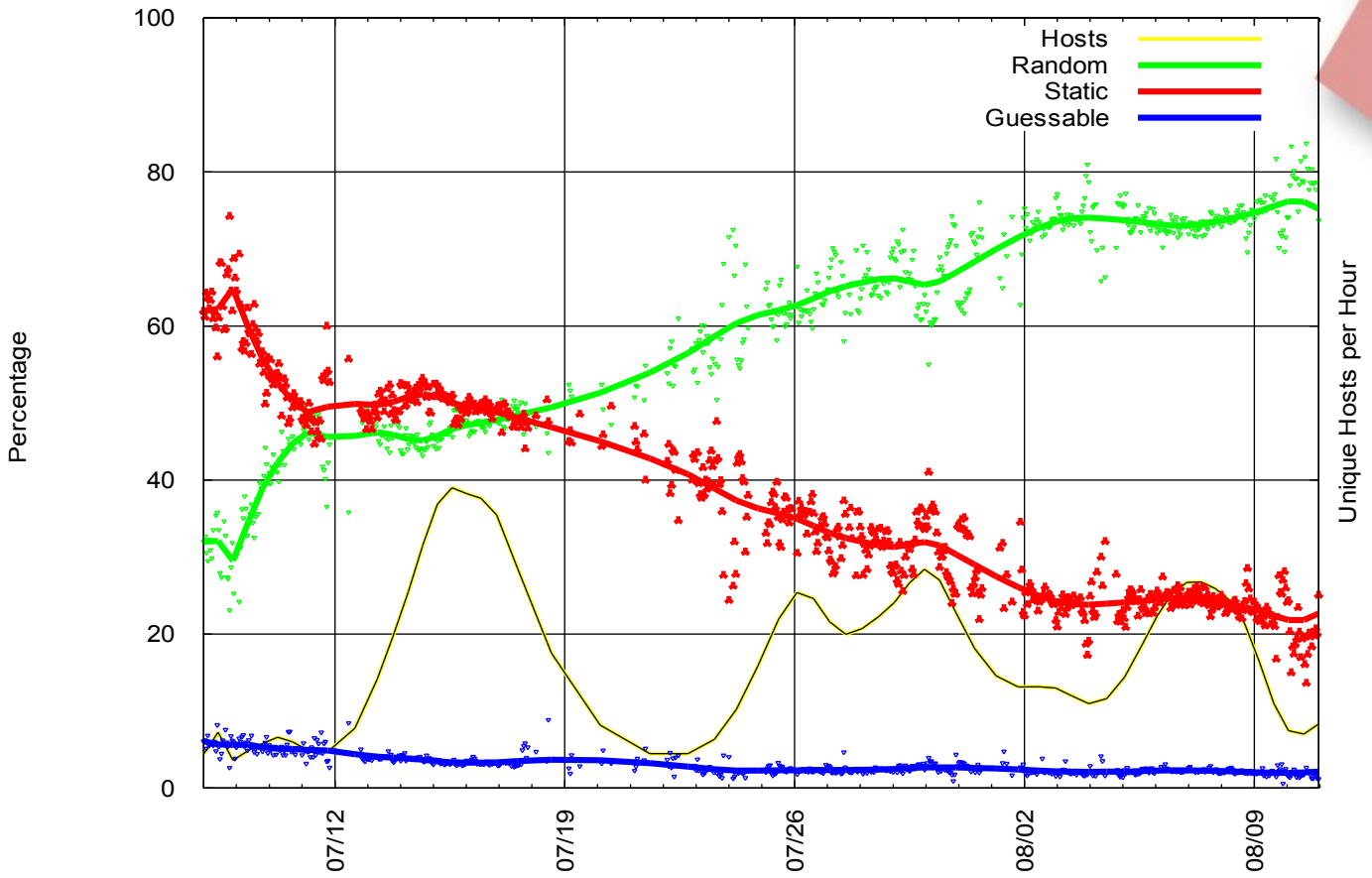
Data from OARC Port Test Tools



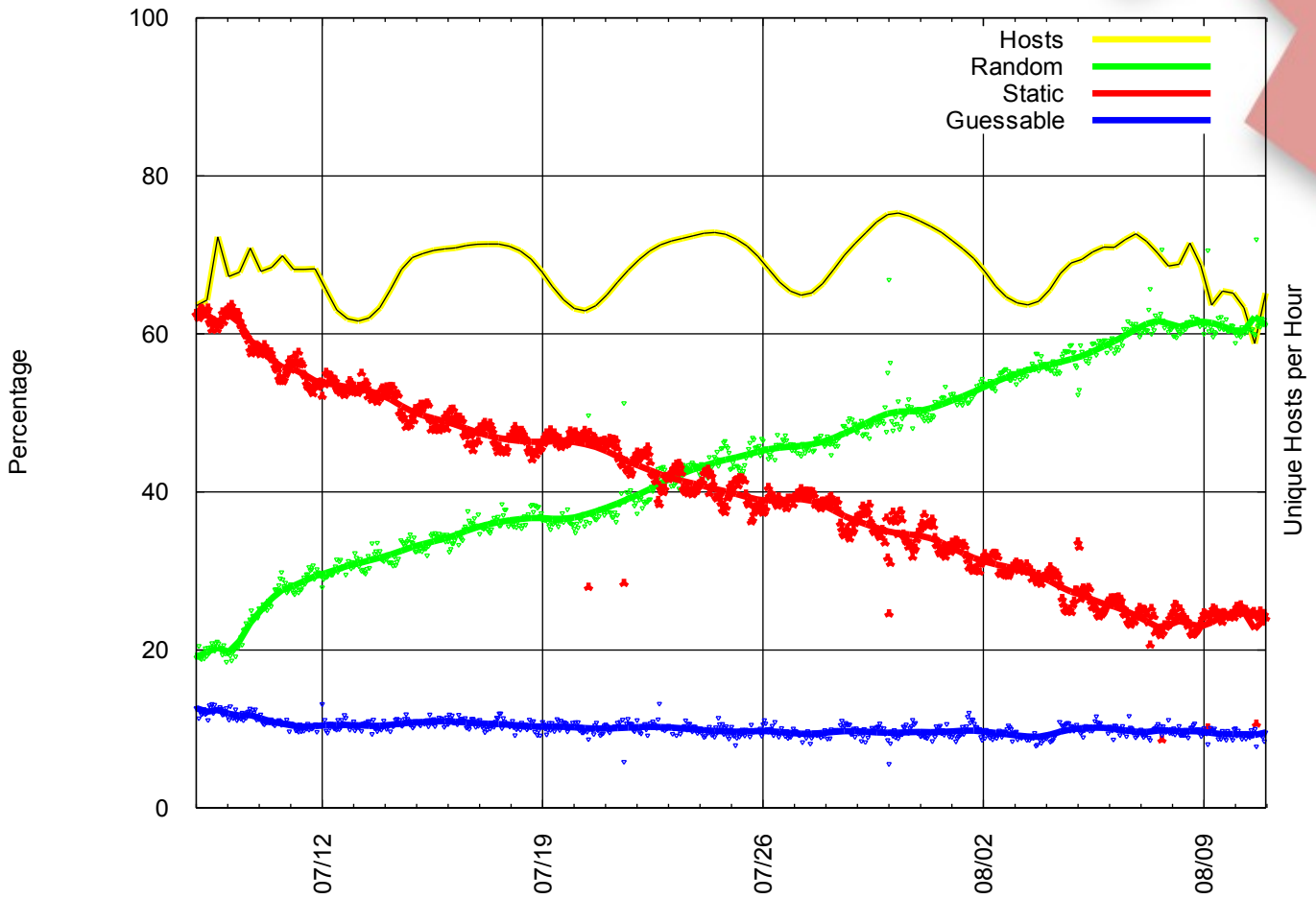
What is ISC SIE ?

- "Secure Information Exchange"
  - provides means for real-time gathering and central re-distribution of security-relevant data
- Initial focus on DNS: data feeds from DNS operators' recursive resolvers
- Sid Faber <sfaber@cert.org> CMU CERT has been analyzing DNS UDP source port data gathered by SIE

CERT SIE Home User Results



CERT SIE Server Results



The Case for DNSSEC

DNSSEC vs port randomization

- there is excellent cause for fear, and no reason to expect that udp port randomization is going to last forever in the face of new threats, both some i've considered or heard of, and others we can only dream of. DNS is too attractive a target, too much fruit hanging too low for too long, to imagine that we'll be crypto-free for our lifetimes.

Paul Vixie

July 10, 2008

DNS-Operations ML

Current fixes are **Interim**

- Source port randomization shifts burden of protecting one application onto the operating system platform
  - can stress OS resources/performance/ portability
- Increasing bandwidth and CPU power will eat away at extra entropy
  - sub-second attacks on unpatched hosts have been demonstrated already
  - a patched host on a gigabit link can still be attacked in as little as 24 hours

Understanding DNSSEC

- DNSSEC enabled authoritative servers provide digital signatures across RRsets in addition to "standard" DNS data
- DNSSEC validating resolvers provide authenticated responses with proven integrity
- Some analogies with website SSL

Understanding DNSSEC

- Clients using validating resolvers get guaranteed "good" data
  - for some value of "guaranteed"
- Data that does not validate provides a "`SERVFAIL`" response from the upstream resolver

Reasons to do DNSSEC

- Effective defense against cache poisoning !
- Great anti-phishing measure
- Interferes with commercial violation of Internet end-to-end principle
  - e.g. Paxfire, Barefruit, Phorm, NebuAd
- General infrastructure integrity enhancement

Obstacles to DNSSEC

- DNS root is not yet signed:
  - US DoC NTIA has not authorized ICANN to do this yet
- Hard to understand/configure
- Difficult to use tools
- CPE equipment issues:
  - http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf

DNSSEC Enablers

- OMB has issued DNSSEC Directive for .gov domains
- DNSSEC Look-aside Validation as interim trust anchor:
  - http://dlv.isc.org
- .se, .br, .museum signed, and other country top-level domains will be soon
- Significant EDNS0 support already
- Easy tools coming in BIND 9.7 release

Conclusions

- Perhaps 25-30% of vulnerable servers still to be patched
- But most were patched within the one-month pre-disclosure window
- Looks like controlled disclosure worked !
- Quality control a challenge when doing multi-vendor synchronized patches..
- But we have only bought ourselves time
- DNSSEC deployment imperative for 2009

Further Information

- Web: http://www.isc.org
  http://www.dns-oarc.org
  https://sie.isc.org
- E-mail: keith_mitchell@isc.org
- Jabber: keith@jabber.isc.org
- Phone: +1 650 423 1348 (EST)

Questions ?