Prevention of DNS Service Disruption
Architecture to Resist DoS

• Authoritative servers typically need to accept queries from every device on the Internet

• A network distributed system places authoritative servers in multiple networks
  – Small scale: different subnets with different gateways
  – Large scale: different Autonomous Systems (AS)

• Geographically distributed systems are in different regions or countries
Types of DoS Protection

• Host authoritative DNS servers at an ISP or Content Distribution Network (CDN)

• Purchase *caching acceleration* service and delegate DNS resolution with a CNAME record
  – Risky because the authoritative server is still needed to provide the CNAME record

• Direct delegation from the TLD to the ISP's or CDN's authoritative servers
  • Better, like Cloudflare
Caching Acceleration

Where is example.com?
example.com is a CNAME for x99.cache.com

Where is x99.cache.com?
x99.cache.com is at 1.2.3.4

Client

SOA DNS Server

Caching Acceleration DNS Server
Project 6x

• Protecting a domain with Cloudflare
Anycast

• Multiple geographically separated servers use the same IP address
• This spreads attacks over the whole network
• Used by the root DNS servers and Cloudflare
NS Delegation

```
Sams-MacBook-Air-2:~ sambowne$ dig samsclass.info ns

;; <<>> DiG 9.8.3-P1 <<>> samsclass.info ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49815
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;samsclass.info.            IN      NS

;; ANSWER SECTION:
samsclass.info.             21600   IN      NS      tom.ns.cloudflare.com.
samsclass.info.             21600   IN      NS      coco.ns.cloudflare.com.
```
Partially Hidden Authoritative Servers

• Some of the authoritative servers are placed behind the firewalls of large ISPs or other organizations
• They act as SOA for only the users of the private network
  • Using BGP to make them preferred
• They are slave servers, updated from the master servers
• This is how UltraDNS works
Figure 48: Placement of authoritative servers in the private access network of an ISP to protect DNS authoritative service from DoS attacks.
UltraDNS DNS Shield

Figure 1 The DNS Shield

- Link Ch 5a
Software

• Whatever you use, keep it updated
• Bind
  – The standard
• djbdns
  – Intended to be more secure than bind, but no longer centrally maintained (links Ch 5b)
• There are many others (link Ch 5c)
DNS Security Extensions
DNSSEC
Purpose of DNSSEC

• Ensure **authenticity** of data origin
• And **integrity** of data received by a resolver from an authoritative DNS server
• Done by signing Resource Record (RR) sets
  – With a private key
  – And including the signature (RRSIG) with the record
Chain of Trust

• Resolver can verify the RRSIG with the server's Public Key
  – Published by the server in its zone file (DNSKEY)
  – Vouched for by the parent zone
  – Vouched for by its parent...
  – Unbroken chain of trust up to the root zone

• Only works if all higher-level zones are signed
DNSSEC Chain of Trust

Root
key self-signed

.org
key signed by root

ietf.org
key signed by .org
Detailed Chain of Trust

<table>
<thead>
<tr>
<th>Owner name</th>
<th>Record type</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.net">www.example.net</a>.</td>
<td>A</td>
<td>example.net.</td>
</tr>
<tr>
<td><a href="http://www.example.net">www.example.net</a>.</td>
<td>RRSIG</td>
<td>example.net.</td>
</tr>
<tr>
<td>example.net.</td>
<td>DNSKEY</td>
<td>example.net.</td>
</tr>
<tr>
<td>example.net.</td>
<td>DS</td>
<td>net.</td>
</tr>
<tr>
<td>example.net.</td>
<td>RRSIG</td>
<td>net.</td>
</tr>
<tr>
<td>net.</td>
<td>DNSKEY</td>
<td>net.</td>
</tr>
<tr>
<td>net.</td>
<td>DS</td>
<td>.</td>
</tr>
<tr>
<td>net.</td>
<td>RRSIG</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>DNSKEY</td>
<td>.</td>
</tr>
</tbody>
</table>

- DS record contains a summary of the DNSKEY record of a child zone
- Link Ch 5d
Root Signed in 2010

July 15, 2010: ICANN publishes the root zone trust anchor and root operators begin to serve the signed root zone with actual keys – The signed root zone is available.

- Link Ch 5e
Demonstration

• `dig rrsig .`
• `dig dnskey .`
  – Shows RRSIG and DNSKEY records for the root
• `dig ds org.`
• `dig dnskey org.`
• `dig rrsig org.`
• `dig dnskey ietf.org`
• `dig rrsig ietf.org`
Root RRSIG Records

Sams-MacBook-Pro-3:~ sambownes$ dig rrsig.

; <<>> DiG 9.10.6 <<>> rrsig.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51794
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:
.

;; ANSWER SECTION:
31952 IN RRSIG SOA 8 0 85400 20181127050000 20181114040000 2134 . 1Y9+ozV9xtCKwSgcQxneZ0X5FB3wCCq3f2m01FwjfUXhX/ysJSSyH67 rcGLMXhsktBwH1iWdRq/XdtSdr5 Dgc8uBI+/Dxh/FA2vUkLowCwpI 6zNaR3WL/03LYDhNgKc+7fZ0Twmn5CT87ZatVpPbufjZkQx+x2wKL+2 V3C1gB gnfLFmCPFqZxRkPNcRZ10Vo3qMhnxwRppVATn7txkHMUXxt2I 0765mYqx2GMC3Ld0BG23FNAB9AkLoHT6A6fBBG4n 4KrIEdZjb7n0RRF qRVjnL/cPHv2PkmU6cSP8XwovWwaP350/qcbW/9nB6n3GfGc8XMGgrnp L5SvGw==
108002 IN RRSIG NS 8 0 518400 20181127180000 20181114170000 2134 . NYFQ8mFyNMhLqFGEfYK3DTs9pbWDBvl0nL6Olv0H4IOYsAZZYgRG0hew hz/9Ggskl1VytU1qvqCwq5aRh31G IVQDKzGzS0swi+i+ggrFynHhihu px28rpqidiFqXXBi/gBMetOuc715KFlyQ4isZ2MA/oB35HuQoyzAh4k JFTs67 LiPkmDvG7KTMc56AGAdvdHws50oHdZEdWz0tUnpSRbF5Zpsz3 99iI0m+5p4nmdMyS7sE62VbD9KFvZnWfrBJQ/ib8 yhlwroKbszVdu5W ytnPsl25EJ0/KrM/51QRgnEYqkipz36GB+zMpdFjKCe19iixiMnMIwz11 zafMrG==

;; Query time: 223 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Nov 14 16:34:13 PST 2018
;; MSG SIZE rcvd: 600
Root DNSKEY Records

```plaintext
; <<< Dig 9.10.6 <<< dnskey .
; ; global options: +cmd
; ; Got answer:
; ; >>>HEADER<<< opcode: QUERY, status: NOERROR, id: 50178
; ; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;; ANSWER SECTION:

; 188002 IN DNSKEY 257 3 0 AwEAaaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkJmgJzjKTOiWlvkIbuzxF3+/4RgwWq7HrxRixhFXex0LAJr5emLvhN75WxgXnLH4+b5xQUNv28q8kvA0MxNroXVOuCaSxIDdDLKkWbd2w9nGe2RGZQCMr3egvLrjy8xWzef0jLxWvN8efS3rcj/EwgvWgb9tarpVUDK/b58dA+sqqls3eNubuv7pr-e0ZG+SrDK6nWeL3c6H5Apzx7LjVc1uTIdSXuuOLYA4/1lbMvSVizU2wDwfRJUfHdY6+c/n8HRFm+z2MBAnXGxw555KrUB5qihyLga8subX2Nn6uWn1R1AkUTY7b4U=

188002 IN DNSKEY 257 3 0 AwEAAdp440E6Mz7c+Vl4spD0lTv20nc85dTW54j0R7D7dSs/zxwxWdJ3QR/ES2VvK000OXLMqyVJSs2YCCSDKuXzxpDPuf--YfAmu8j7lzYYdWTGvwyAHzEaExTMqMjiKYB96pW6cRkgk2Dns2vvo/PxW9qKQsylbtd8PcwWgllHgReBvP 7kEv/Dd+3b3YmAkt4jNqDdAySg558Zld+c9eGxkgwo0iuh4GqRkf stHx1ipreo5HcZuh380aw1UsT4y3eT8U/3RGTOSL8/8Ftirux/h297o57 tCcwSPt0wryy30FNTLffMo8v7WGuogfkg8hPfP7TTKHI2bLWen5CRsv YsQbKyGpF78=

188022 IN DNSKEY 257 3 0 AwEAaaz/AIKVzrpC6iA7gEzahoR+9W29cuxhJ3hWLOyqB5E W0dBgcCjFVQUTf6v5BFJlwB0vY1BEzrAc0qBGcz/RStIoD8gQnflL2MTJrKkoxX bdfaeVePDvYHmeg37NWAJ09vMvXp/VHL496M/DDxkje5/Ffucp2gAaD X6R56CSpxyY6BLSvPwVjR0Z5wzz1apAzvN9dlzEhecX71CBBtuAtG31D0pZ W5h0A2hxCTMjJPJ31BqF6dsV6 DoB0zggu0sGlcG60y7olYQDx75relS Qagecu+ipADTTJ25AsRTxup1BQNGCLmqra=RLKB1p1dfwYB4N7knNulq QxA+Uk1hHz0=

;; Query time: 436 msec
;; SERVER: 172.20.18.1#53(172.20.10.1)
;; WHEN: Wed Nov 24 16:35:34 PST 2018
;; MSG SIZE rcvd: 853
```
Top-Level Domain: org.
DNSSEC of Top-Level Domains

Nov. 2013

- 332 TLDs in the root zone in total
- 135 TLDs are signed;
- 129 TLDs have trust anchors published as DS records in the root zone;
- 3 TLDs have trust anchors published in the ISC DLV Repository.

Nov. 2016

- 1509 TLDs in the root zone in total
- 1360 TLDs are signed;
- 1349 TLDs have trust anchors published as DS records in the root zone;
- 5 TLDs have trust anchors published in the ISC DLV Repository.

Nov. 2018

- 1535 TLDs in the root zone in total
- 1400 TLDs are signed;
- 1391 TLDs have trust anchors published as DS records in the root zone;
- 0 TLDs have trust anchors published in the ISC DLV Repository.

Link Ch 5f
Why DNSSEC deployment remains so low

By Taejoong Chung on 6 Dec 2017

• Link Ch 5m

<table>
<thead>
<tr>
<th>Registrar (Domain of Auth. Nameservers)</th>
<th>Domains (All)</th>
<th>Domains (With DNSKEY)</th>
<th>DNSSEC Supp (Regis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy (domaincontrol.com)</td>
<td>37,652,477</td>
<td>8,139</td>
<td></td>
</tr>
<tr>
<td>Alibaba (hichina.com)</td>
<td>4,292,138</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Registrar (Domain of Auth. Nameservers)</td>
<td>Domains (All)</td>
<td>Domains (With DNSKEY)</td>
<td>DNSSEC Support (Registrar)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>GoDaddy (domaincontrol.com)</td>
<td>37,652,477</td>
<td>8,139</td>
<td>✓</td>
</tr>
<tr>
<td>Alibaba (hichina.com)</td>
<td>4,292,138</td>
<td>3</td>
<td>×</td>
</tr>
<tr>
<td>1AND1 (1and1)</td>
<td>3,802,824</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>WordPress (wordpress.com)</td>
<td>888,174</td>
<td>3</td>
<td>×</td>
</tr>
<tr>
<td>Amazon (aws-dns)</td>
<td>865,065</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>Xinnet (xincache.com)</td>
<td>836,293</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>Google (googledomains.com)</td>
<td>813,945</td>
<td>1,945</td>
<td>×</td>
</tr>
</tbody>
</table>
DNSSEC Is Dead, Stick a Fork in It
By: Larry Seltzer | December 16, 2007

Opinion: If political battles weren't preventing DNSSEC from being used seriously on the Internet, we'd have to deal with the fact that the major resolvers would reject it and that technical problems would make it unsatisfying.

- Link Ch 5n
Cloudflare Looks to Take the Pain Out of DNSSEC Protocol Adoption

Larry Loeb, Author, 9/21/2018

Cloudflare is adding a new feature to its hosting and firewall products that the networking company hopes will address the slow uptake of the Domain Name System Security Extensions (DNSSEC) protocol.

The method to support the DNSSEC protocol has been a manual one before this, requiring a website owner to add a "DS record" to its account with their registrar.

A Cloudflare customer that is working with a registry that supports DNSSEC can activate it for their account by the press of a button from the Cloudflare dashboard.

• Link Ch 5o
DNSSEC Validator
Browser Extension

• Link Ch 5j
DNS-based Authentication of Named Entities (DANE)

- Uses DNSSEC to validate SSL certificates, not Certificate Authorities
- Link Ch 5k
DNSSEC Issues

• Protocol still changing
• Only secures record to resolver, not traffic from resolver to client
• Another reason to disallow external DNS servers like 8.8.8.8
  – To keep all resolver traffic local
Authenticated Denial of Existence

• There is no fred.ccsf.edu
  – Three systems to prove that
• NXT record (1999); insecure & replaced by
• NSEC record (2005); insecure & replaced by
• NSEC3 record (2008)
• All incompatible with one another
Transaction Signatures: TSIG

• Maintains integrity of DNS messages between two servers
• Cryptographically signs messages with TSIG
  – Calculates a Message Authentication Code
  – Encrypts it with a secret key
  – Key shared by the two end-nodes
  – Includes the time, to prevent replay attacks
  – TSIG expires after the "time fudge factor"
• You must generate secret key and securely transmit it to the other server
Transaction Signatures: TSIG

- Originally used MD5 only, but now also uses SHA-1 and SHA-256
- Error messages include BADKEY, BADSIG, and BADTIME
- Error messages are unsigned
  - They can be spoofed, resulting in DoS
Transaction Signatures: SIG(0)

• Alternative signature method using public key cryptography
• Public key stored in a KEY record
Transaction Keys (TKEY)

- Establishes a shared secret using
  - Diffie-Hellman key exchange, or
  - General Security Service API (based on Kerberos)
- TKEY record contains the keying material required
- Vulnerable to man-in-the-middle attacks
  - Should be secured with SIG(0) (shared secret)
Software Diversification

• Most root servers use Bind
• K and H servers use NSD from NLnetlabs
Master-Slave Setup

- Changes are made at the master
- Replicate to the slaves
- Slaves can be masters of lower-level slaves
Configuring a Slave Server in Bind

```plaintext
zone "packetproof.com" IN {
    type slave;
    file "db.packetproof.com.bk";
    masters {184.106.196.10;};
};
```
Limitation of 512 Bytes

• Running many slave servers is good for fault-tolerance
  – But they all need to be listed as authoritative servers in DNS responses
  – Limited to 512 bytes in legacy systems

• Failover via multiple NS records is slow
  – Requires several seconds for timeout of a bad server
CCSF.EDU has 4 NS Records on 4-28-15

<table>
<thead>
<tr>
<th>QUESTION SECTION:</th>
<th>IN</th>
<th>NS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccsf.edu.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ANSWER SECTION:</th>
<th>IN</th>
<th>NS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccsf.edu.</td>
<td>18342</td>
<td>NS  ns3.ccsf.edu.</td>
</tr>
<tr>
<td>ccsf.edu.</td>
<td>18342</td>
<td>NS  ns4.cenic.org.</td>
</tr>
<tr>
<td>ccsf.edu.</td>
<td>18342</td>
<td>NS  ns6.cenic.org.</td>
</tr>
<tr>
<td>ccsf.edu.</td>
<td>18342</td>
<td>NS  ns5.cenic.org.</td>
</tr>
</tbody>
</table>
Automatic Failover

• Use a load balancer
• Appears to be a single server to external nodes
Protection of DNS Service
Firewalls, IDS/IPS

- Run on hardened systems
- Port 53 UDP/TCP open
- Management ports only open to internal hosts
- IDS/IPS blocks known attacks by signatures
- Firewalls limit traffic with Access Control Lists (ACLs)
- Older firewalls limit DNS packets to 512 bytes
  - Now obsolete; EDNS allows UDP packets up to 4096 bytes (link Ch 5i)
Scrubbers

- DDoS attacks look like many legitimate customers
- Scrubbers block packets that meet DDoS criteria
  - Not usually fully automated
- When under attack, BGP updates are sent to redirect traffic to the scrubbers
Normal Networking
Using Scrubbers
Service Monitoring and Restoration
Monitoring

• Send periodic probes from multiple ISPs and geographic regions
  – Such as DNS requests
  – Send directly to monitored servers
  – Verify that responses are accurate
Backups

• Regular backups of the DNS servers are essential
• Can be full or incremental
• Could back up whole OS, or just DNS configuration files
• Cloud DNS servers must be backed up too
  – Using backup tools appropriate for the cloud service
• MUST TEST YOUR BACKUPS
Slow DNS Response

• If a DNS server is down, it slows responses
• Because the dead server must time out before another server is queried
• Remove NS and A records for failed server to avoid this