about:mozilla
Agenda

• The Basics
• Implementation
• What we I messed up
What and the Why

• DNS Security Extensions
  • Based on public key crypto
  • rfc 4033
  • http://en.wikipedia.org/wiki/DNSSEC
• DNS wasn’t created for today’s world
  • DNS cache poisoning
What’s new?

- 4 new RRs - rfc 4034
  - DNSKEY
  - DS
  - NSEC/NSEC3
  - RRSIG
What's new?

- Keys - Public and Private
  - Key Signing Key - KSK
  - Zone Signing Key - ZSK
- Algorithms
- Rollovers
- Operational Practices - rfc 4641
# Relationships

## Debugging DNSSEC problems for mozilla.org

<table>
<thead>
<tr>
<th>Domain</th>
<th>DNSKEY Records</th>
<th>RRSIGs</th>
<th>Additional Details</th>
</tr>
</thead>
</table>
| .              | Found 3        | 1      | DRSIG=19036/SHA1 verifies DNSKEY=19036/SEP
|                | DRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
|                | . refers to org for mozilla.org
|                | Found 2 DS records for org in the referral
|                | Found 1 RRSIGs over DS RRset
|                | RRSIG=21639 and DNSKEY=21639 verifies the DS RRset
| org            | Found 4        | 2      | DRSIG=21366/SHA256 verifies DNSKEY=21366/SEP
|                | DRSIG=1743 and DNSKEY=1743 verifies the DNSKEY RRset
|                | org refers to mozilla.org for mozilla.org
|                | Found 1 DS records for mozilla.org in the referral
|                | Found 1 RRSIGs over DS RRset
|                | RRSIG=1743 and DNSKEY=1743 verifies the DS RRset
| mozilla.org    | Found 3        | 2      | DRSIG=51618/SHA1 verifies DNSKEY=51618/SEP
|                | DRSIG=51618 and DNSKEY=51618/SEP verifies the DNSKEY RRset
|                | mozilla.org A RR has value 63.245.209.11
|                | Found 1 RRSIGs over A RRset
|                | RRSIG=62897 and DNSKEY=62897 verifies the A RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test mozilla.org at [dnsviz.net](http://dnsviz.net).
Before you leap...

• Check if your TLD has been signed
  • Else you’re an Island of Trust
• Check with your registrar about DNSSEC
  • You might have to poke a bit
  • http://bit.ly/dnssecorg
• Make sure your software works
  • bind, unbound, opendnssec
Setup - Before

DNS configs

Source Control

ns1.mozilla.org

ns2.mozilla.org

ns3.mozilla.org
Setup - After

Diagram showing the setup after with various components connected including DNS configs, Source Control, Signer, and Internet.
Commands

Generate keys

```
dnssec-keygen -K /mozilla.org/ -3 -n ZONE -f KSK mozilla.org
dnssec-keygen -K /mozilla.org/ -3 -n ZONE mozilla.org
```

Modify times (if needed)

```
dnssec-settime -A +6mo <keyid>
```

Sign your zones

```
dnssec-signzone -S -K /mozilla.org/ -o mozilla.org -a -t -u -3 salt -H 1 mozilla.org
```

Changes to bind - named.conf

```
dnssec-enable yes;
dnssec-validation yes;
zone "mozilla.org" IN {
    type master;
    file "mozilla.org.signed";
}
```
Steps

• Upgrade bind across the board
• Kick off signer
• DNS servers pick up changes and restart
• Profit!!oneone!!
Verify!
Things to be aware of

- Keys are everything, protect them
- Make sure you have a backup plan
- Eventually, you run the risk of your entire domain being unreachable
- Sign (zones), publish (zones) then push (DS)
- Network equipment might need changes
boo-boo(s)

• DS was live, no signed zones aka “Security Lameness”
• Log levels
• Of course, everyone on twitter notices and #fails you.
boo-boo(s)
Thanks!