# My Life with the Mob


Michael Sinatra

University of California, Berkeley

# What's DLV?

- DNSSEC Lookaside Validation
  - Allows for DNSSEC validation without signed root or TLDs.
  - Uses DLV RRTYPE which is of the similar format to the DS record.

# What's DLV?

- See:
  - RFC 4437
  - Joao Damas's presentation at NANOG 37:
    http://nanog.org/meetings/nanog37/abstracts.php?pt=Mzg1Jm5hbm9nMzc=&nm=nanog37
  - At least two implementations support it:
    - BIND (>=9.3.3)
    - unbound (>=1.1.0)

# Why use it?

- Allows for early deployment of DNSSEC.
- Why be an early deployer?

# Why use it?

- All I needed to know I learned on the New York City Subway.

# Why use it?

- Yes there is risk:
  - Research universities should still be willing to be on the bleeding edge.
  - Risk should be reasonable.
  - There is recognition at UC Berkeley that we have had a role in the development of the Internet and we shouldn’t (have) abandon(ed) that role.

# What did we do?

- Began testbed DNSSEC validation with Internet Systems Consortium (ISC) DLV around the time of the Kaminsky announcement.
- October 2008: Put into production.
- All UC Berkeley's centrally-maintained caching resolvers perform DNSSEC validation using ISC DLV.

# How did it work?

- Surprisingly well.
- Three failures in 6 months.
  - GOV NSEC3 validation
    - This was a BIND (<9.6.0) coding issue (now fixed). unbound already supports NSEC3.
  - Signing issues (the first one was a doozy)
    - (didn’t get too much flak, though)
    - This is a basic DNSSEC issue, not a DLV issue

# Why DLV and not TAR?

- Controversies:
  - “DLV is a stunningly bad idea because it implies that I, as a caching server operator, would need to share fate with ISC's DLV infrastructure from polices to processes to software to hardware over all of which I'd have no control and I'd have to share that fate _in real-time_. You guys screw up, I lose instantly.”
    - David Conrad

# Why DLV and not TAR?

- Controversies:
  - “though i understand that isc means well with dlv, and is trying to paste over a politcal farce with a technical patch, the dlv trust model is essentially broken.  it moves signed root trust from the iana to isc, and, aside from the fact that this very change is serious breakage, isc's trust process and policies are unclear.”
    - Randy Bush

# Why DLV and not TAR?

- Controversies:
  - “While it is easy to choose a different search engine and most users can be reasonably be expected to deal with the fact if/when Google went down, I have some skepticism that (say) your average art student at UCB would have a clue as to how to change the caching name server they point to (if they are even able to).”
    - David Conrad

# Why DLV and not TAR?

- I made the conscious decision to trust ISC.
- I vetted that decision with IT staff at the university.
- I still bear responsibility for decisions I have made regarding DNS.
- See:

https://lists.dns-oarc.net/pipermail/dns-operations/2009-April/003773.html

# Alternatives/Improvements?

- DLV features
  - Allow zone transfers
- Other alternatives
  - Use DLV records to derive DNSKEYs and create your own trust anchor repository--still outsourcing trust and key management to ISC (or someone else).
  - Build TAR from IANA and/or others.
    - Scripts to do this already exist.
    - There’s still stuff that can go wrong.

# Alternatives/Improvements?

- DLV features
  - Allow zone transfers
- Other alternatives
  - Use DLV records to derive DNSKEYs and create your own trust anchor repository--still outsourcing trust and key management to ISC (or someone else).
  - Build TAR from IANA and/or others.
    - Scripts to do this already exist.
    - There’s still stuff that can go wrong.

# What Have I Learned?

- Many more failure modes.  (Well, I expected that.)
- Firewalls are a pain in the a$$.  (Oops, I already knew that.)
- What happens when the key for your {dlv,root} zone expires in your local TAR.
- What happens when the {dlv,root,<your-domain-here>} zone is “incorrectly” signed.
- People are willing to accept some risk if they think that there will be gains in the future.
- CPU/bandwith load has not *yet* been significant.

# So long and thanks for all the Tastykakes!

Nobody bakes a kake as tasty as
a Tastykake.