OpenDNSSEC
Error recovery

UNIVERSITEIT VAN AMSTERDAM

Aleksandar Kasabov

Research project II

July 5th, 2012

NLnet Labs

Outline

- OpenDNSSEC (ODS)
- Key rollovers test
- Error recovery
  - Environment changes
  - Components crash
- What are the “best” TTL settings
- Summary
- Q&A

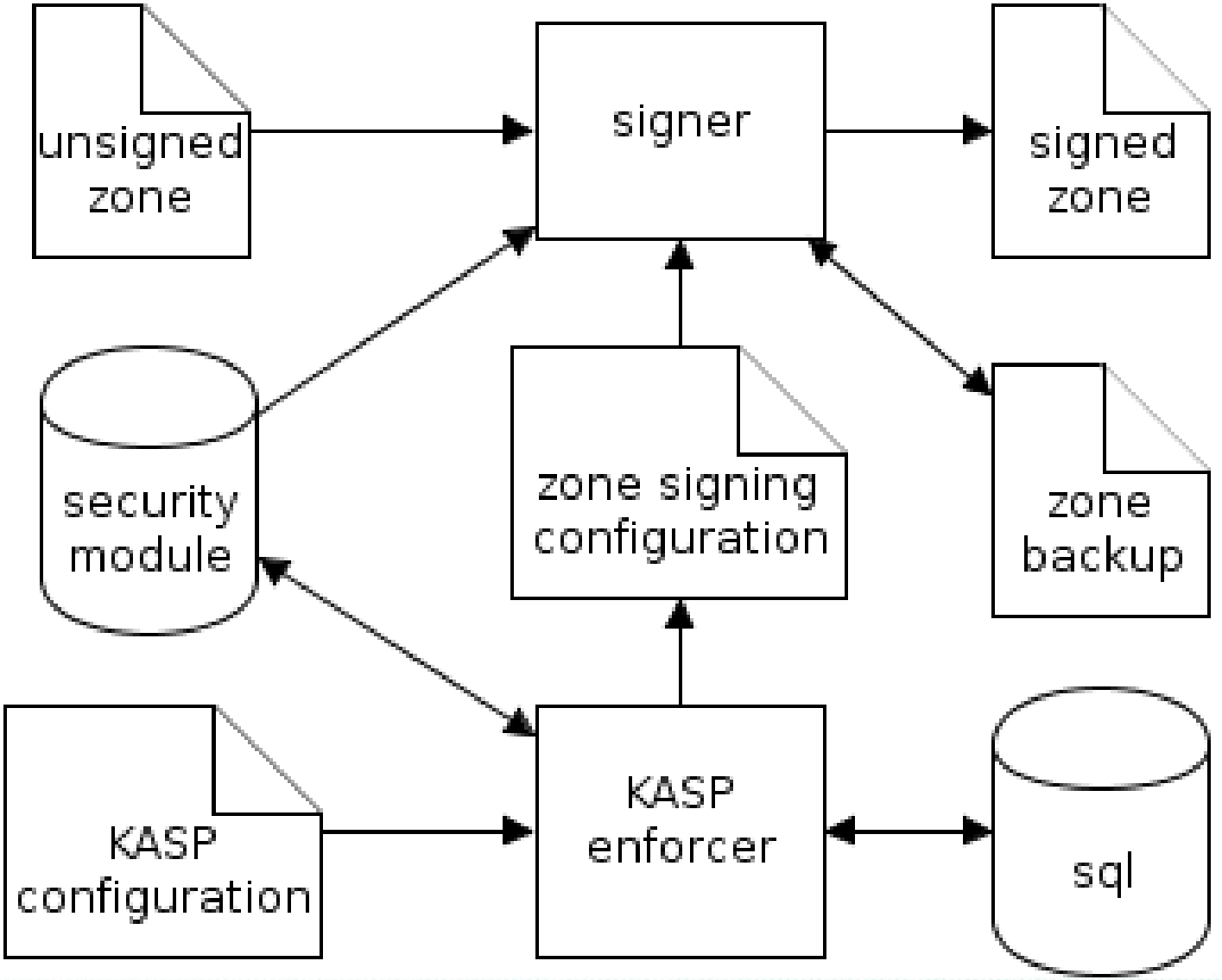
OpenDNSSEC

General info

- Open source turn-key solution for DNSSEC
  - Automatic key management
  - Resilience
- Collaborators
  - .SE (The Internet Infrastructure Foundation), Kirei, NLnet Labs, Nominet, SIDN, Sinodun Internet Technologies, SURFnet
- Investigated versions
  - 1.4.0a2
  - 1.5.0a1 aka 2.0 aka NG

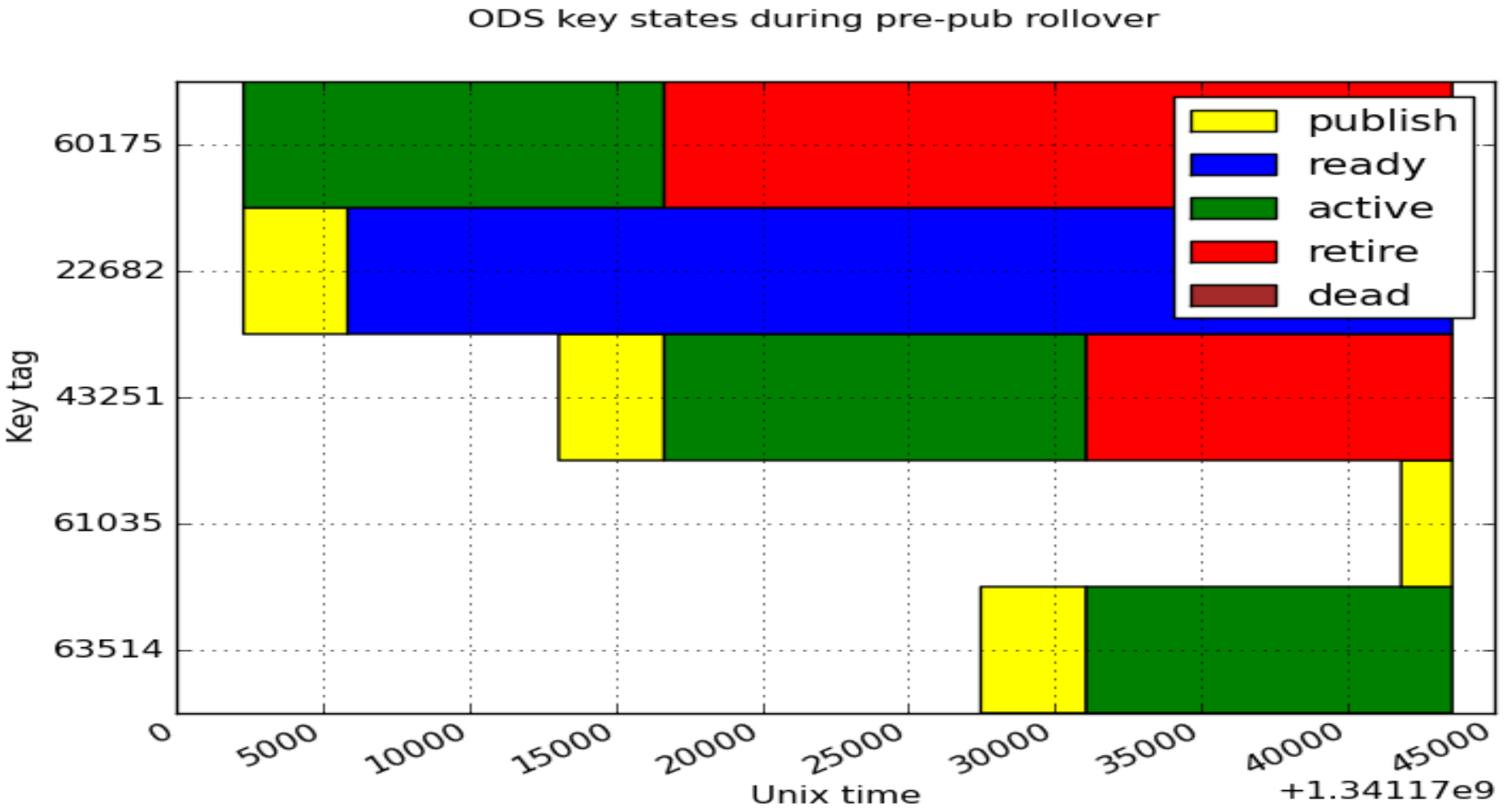
OpenDNSSEC (2)

Architectural design



NLnet Labs

Key rollovers tests
ZSK key rollover with ODS 1.4



NLnet Labs

Error recovery

Environment changes: files

- User updates/deletes a signed zone file
- User updates a zone signing configuration file
- ODS could watch signed zone files
  - Verify signed zone files (e.g. validns*, credns)
  - Verify zone signing configuration files against the policy settings
- ODS should NOT allow changes to
  - signed zone files
  - zone signing configuration files

* http://validns.net

Error recovery (2)

Environment changes: system date

- System date changes before the start of ODS
  - Old signed zone files do not = bogus zone
- ODS should
  - Check system date upon startup
  - Resign zones if date changed
  - Use central NTP service

```
root@debian:~/$ ods-signer queue
It is now Wed Jun 13 14:39:32 2012
I have 1 tasks scheduled.
On Thu Jun 13 00:11:04 2013 I will [sign] zone example.com
```

Error recovery (3)

Components crash: HSM

- Lost keys
  - manual user mistake
  - HSM is replaced
- ODS should introduce new keys (on time)

```
Jun 14 15:14:11 nsi ods-signerd: [hsm] unable to get
key: key 6a0f4d427f6f844b981a965a9e7adb4b not found
Jun 14 15:14:11 nsi ods-signerd: [zone] unable to publish
dnskeys for zone example.com: error creating dnskey
Jun 14 15:14:11 nsi ods-signerd: [tools] unable to read zone
example.com: failed to publish dnskeys (General error)
Jun 14 15:14:11 nsi ods-signerd: [worker[4]] backoff task
[configure] for zone example.com with 60 seconds
```

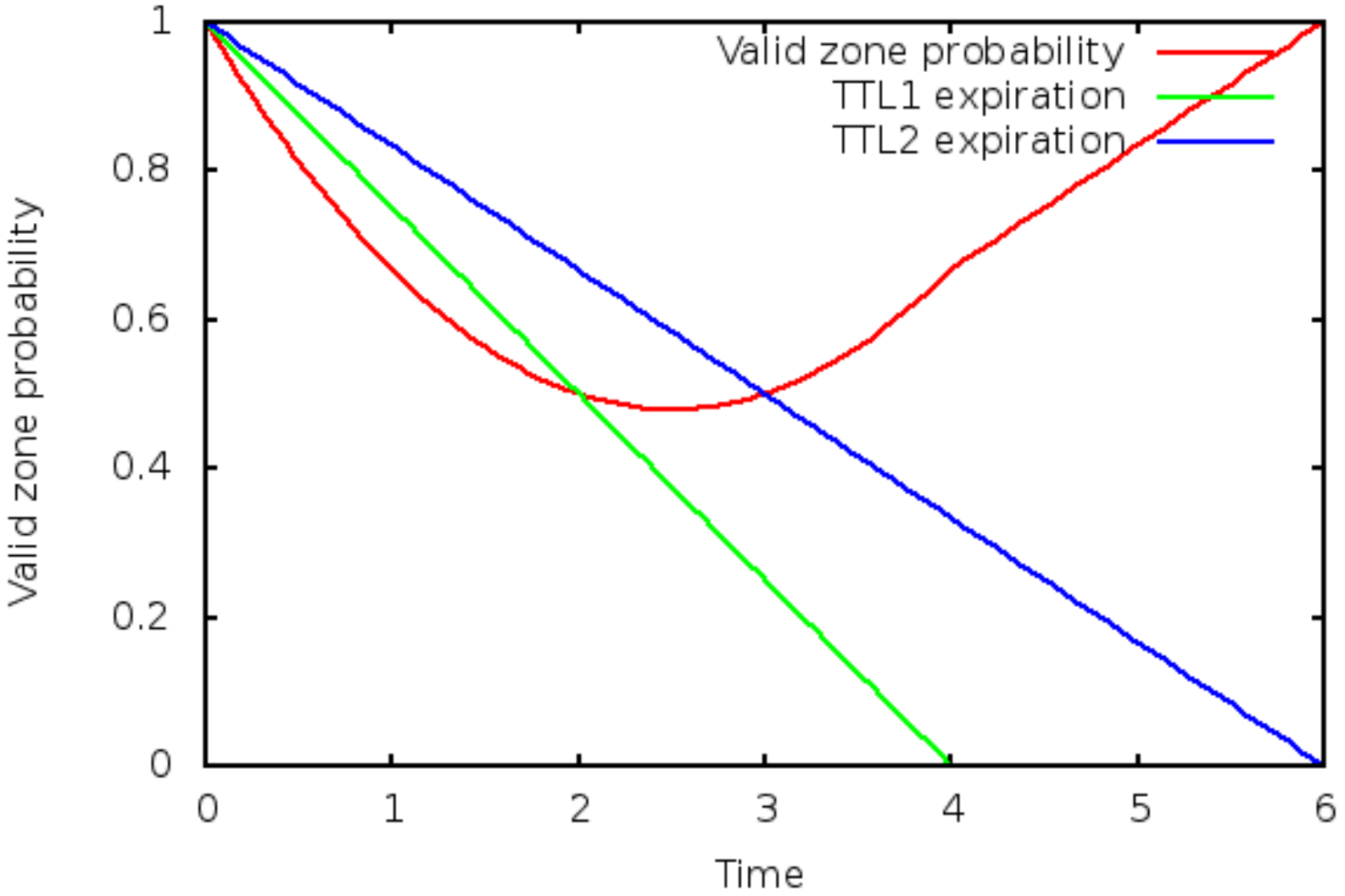
Error recovery (4)

Components crash: Signer

- Not much can be done to recover
  - Restart the signer
  - Enforcer might have rolled new key
- What TTL values minimize the impact of a crashing signer?
- Case assumptions in order to generalize
  - A very very popular zone
  - Records are cached uniformly in validators

Error recovery (5)

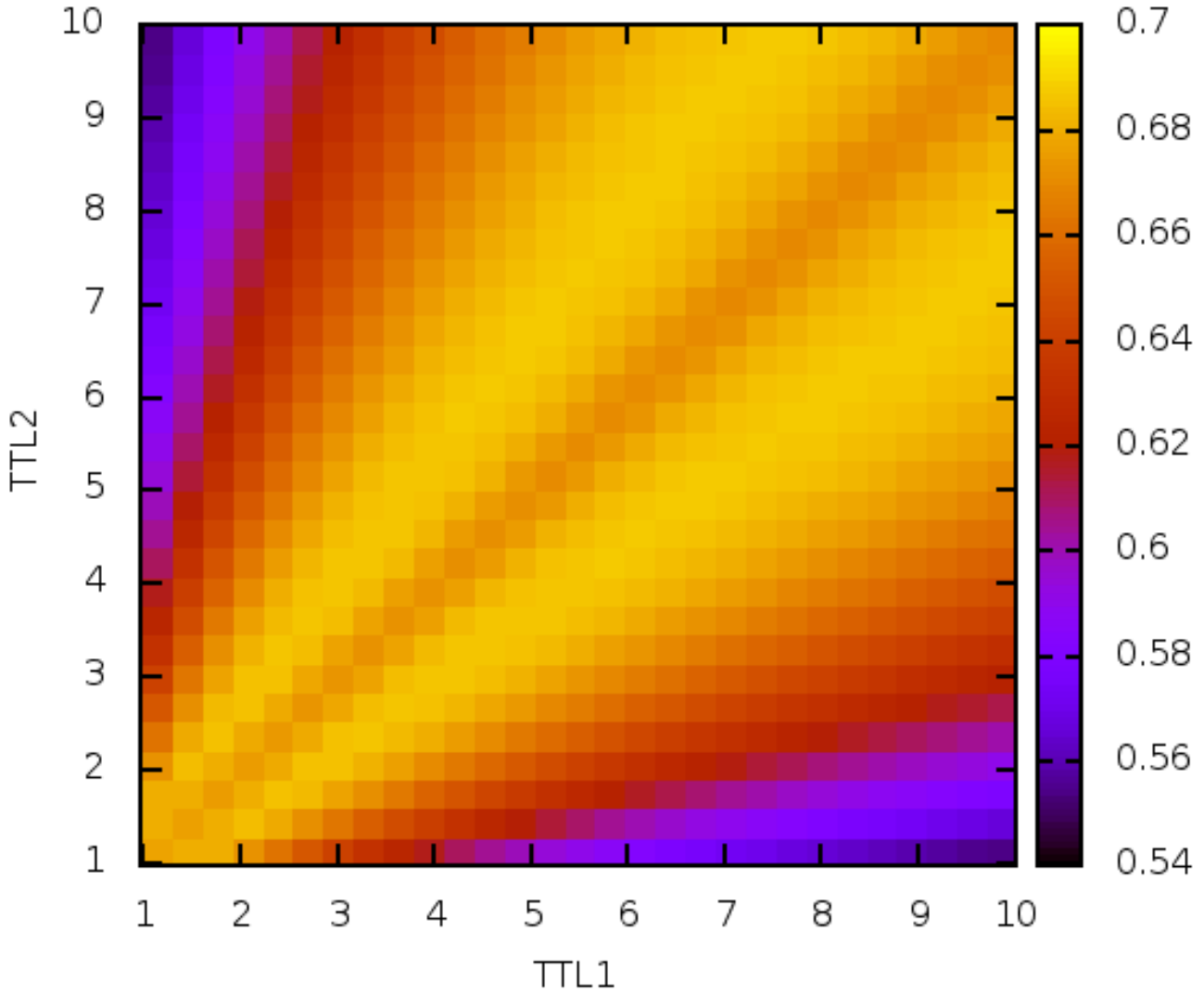
Signer crash: probability of zone validity for TTL1=4, TTL2=6



NLnet Labs

Error recovery (6)

Signer crash: zone validity probability for any TTL combination



NLnet Labs

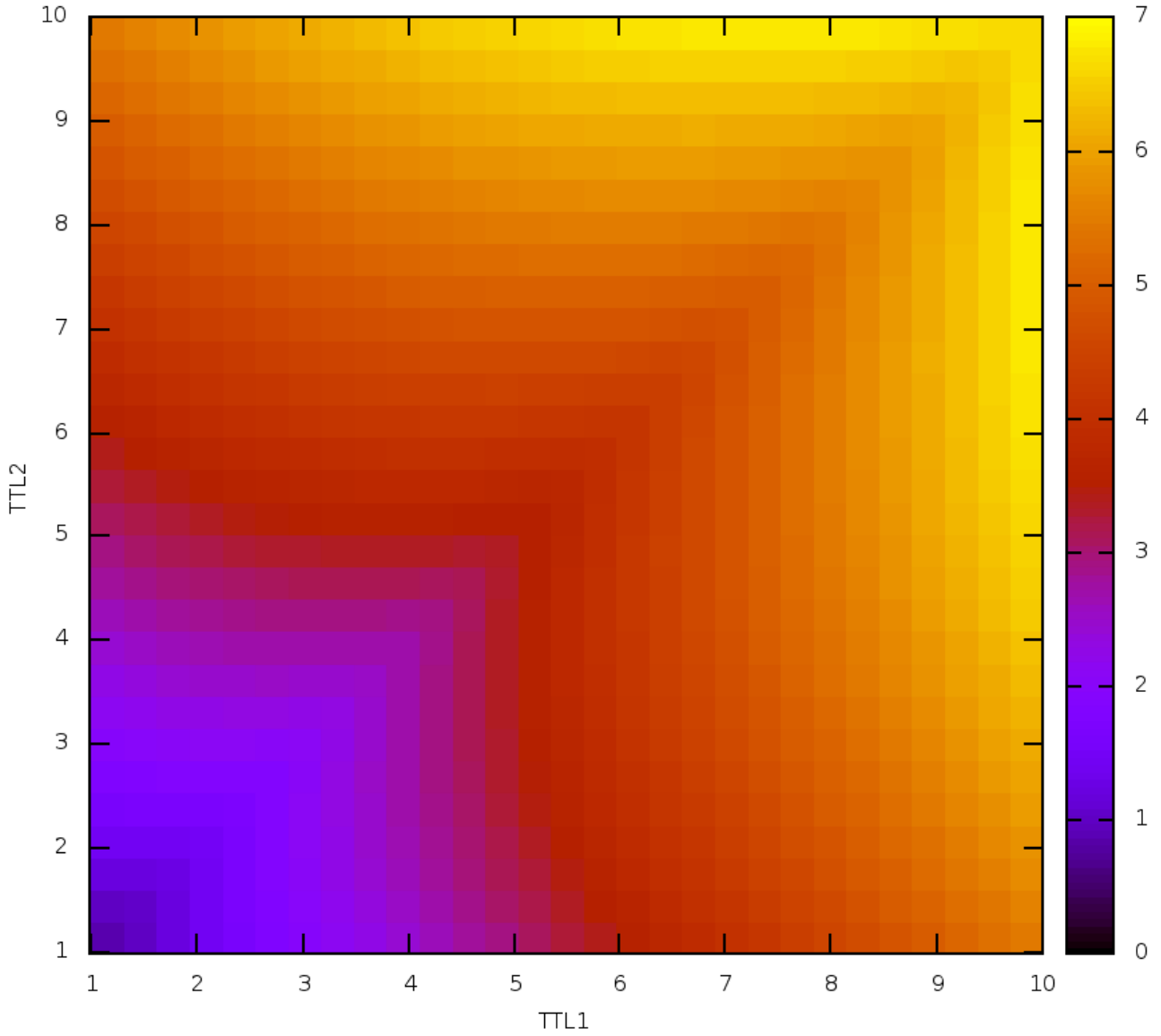
Summary

- Recommendations
  - Use NTP service instead of system date
  - Watch for file changes
  - Losing keys is not fatal (if noticed on time)
  - TTL1 = ¾ TTL2
- Future work
  - Test key algorithm rollovers
  - Signer + Enforcer as one daemon?
  - Explain the “¾ TTL” relationship

Questions round

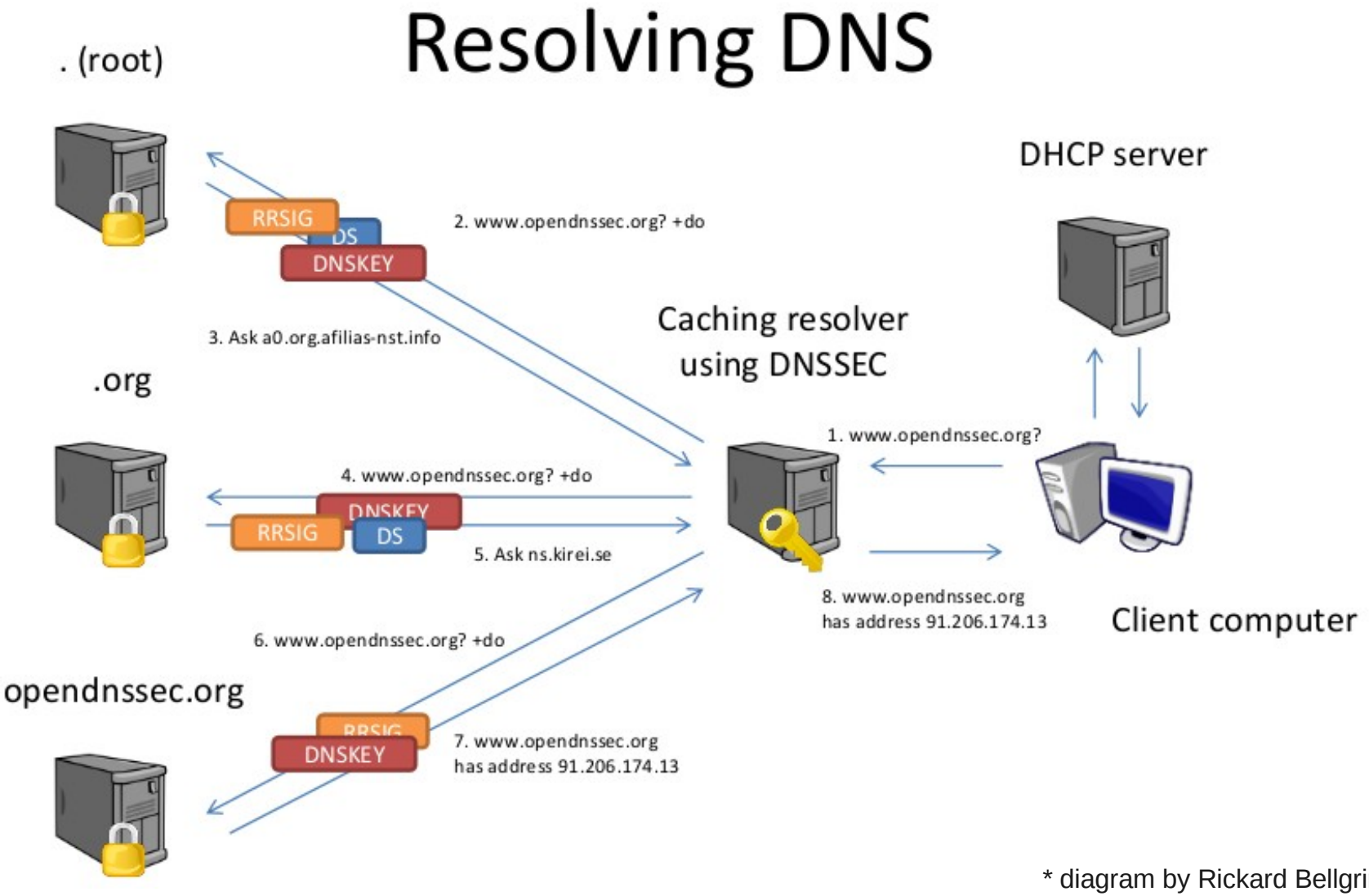
- Acknowledgements
  - Yuri Schaeffer
  - NlnetLabs
- Questions

Signer crash: zone validity absolute probability for any TTL combination



NLnet Labs

DNSSEC



* diagram by Rickard Bellgrim (iis.se)

NLnet Labs