UNBOUND

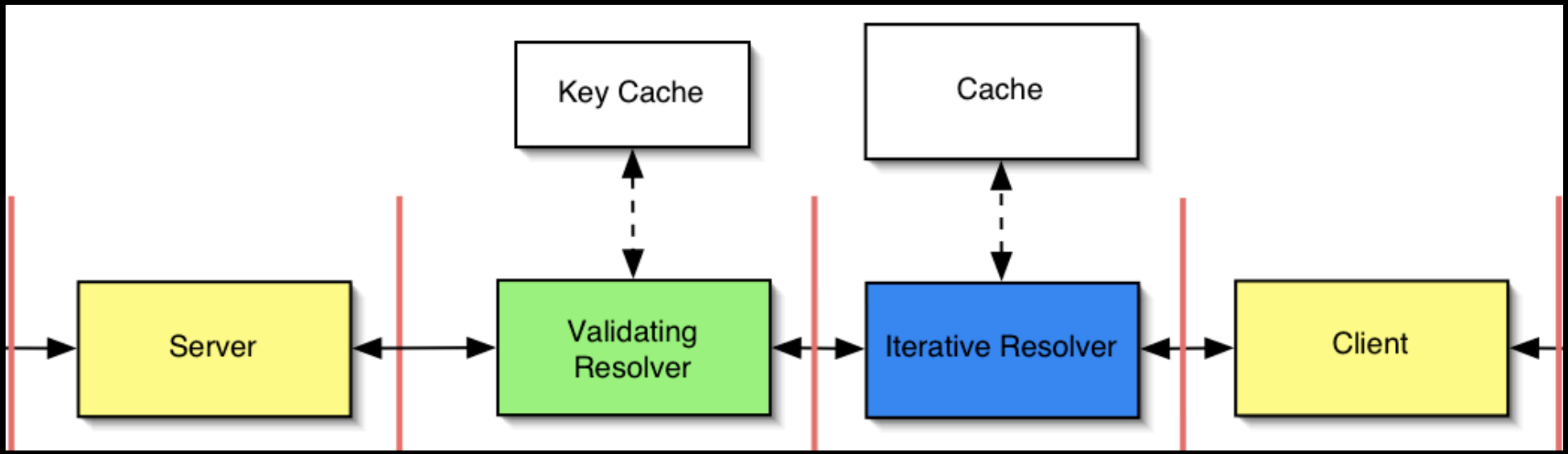
a validating caching resolver

Brett Carr, Nominet

history

- 2004 modular design
  - Nominet/Kirei/EP.net
- 2005 JAVA based prototype
  - Verisign
- 2006 C based production code
  - NLnet Labs, you know, NSD & ldns

modules


Key Cache
Cache
Server
Validating Resolver
Iterative Resolver
Client

Why a new resolver

- code diversity
- IETF “running code” requirement
- Alternative validator

Target

- Workgroup local DNS resolvers
- Large caching resolver installations
- Validating library (libunbound) for apps

Support

- Supported by NLnet Labs.
  - not for profit, public benefit foundation
- 2 year change notice.
- Version 1.0.0 released May 2008
- Version 1.0.2 released August 2008
- get it at http://unbound.net

Basic Features

- Recursion
  - v4/v6 dual stack support
  - Access control
- DNSSEC validation
  - includes NSEC3 plus opt-out
- Caching

additional features

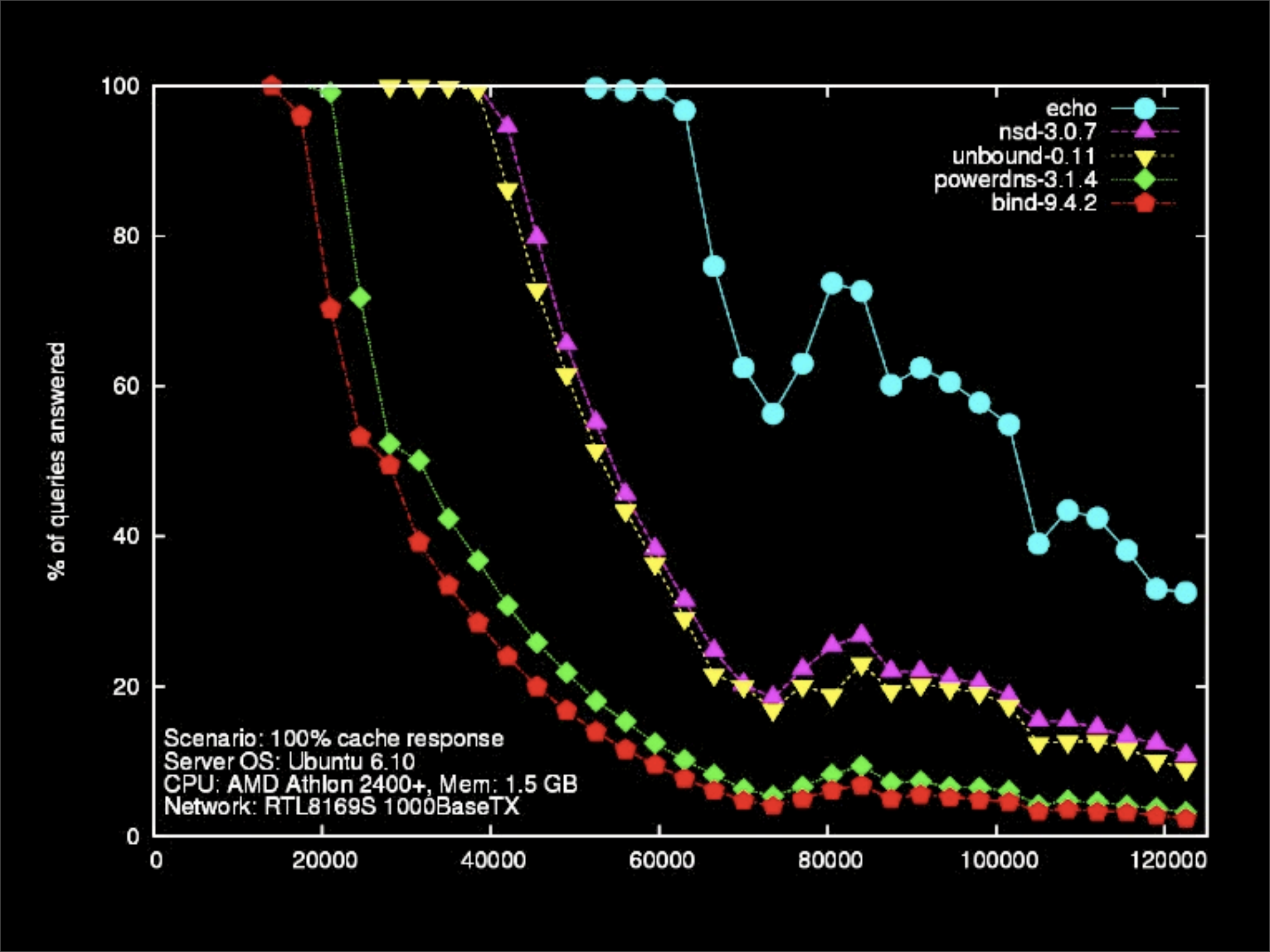
- optional thread support
- trust anchor configuration
  - rb-tree for trust anchors
- No authoritative server, but:
  - will serve localhost/1918
  - can block domains

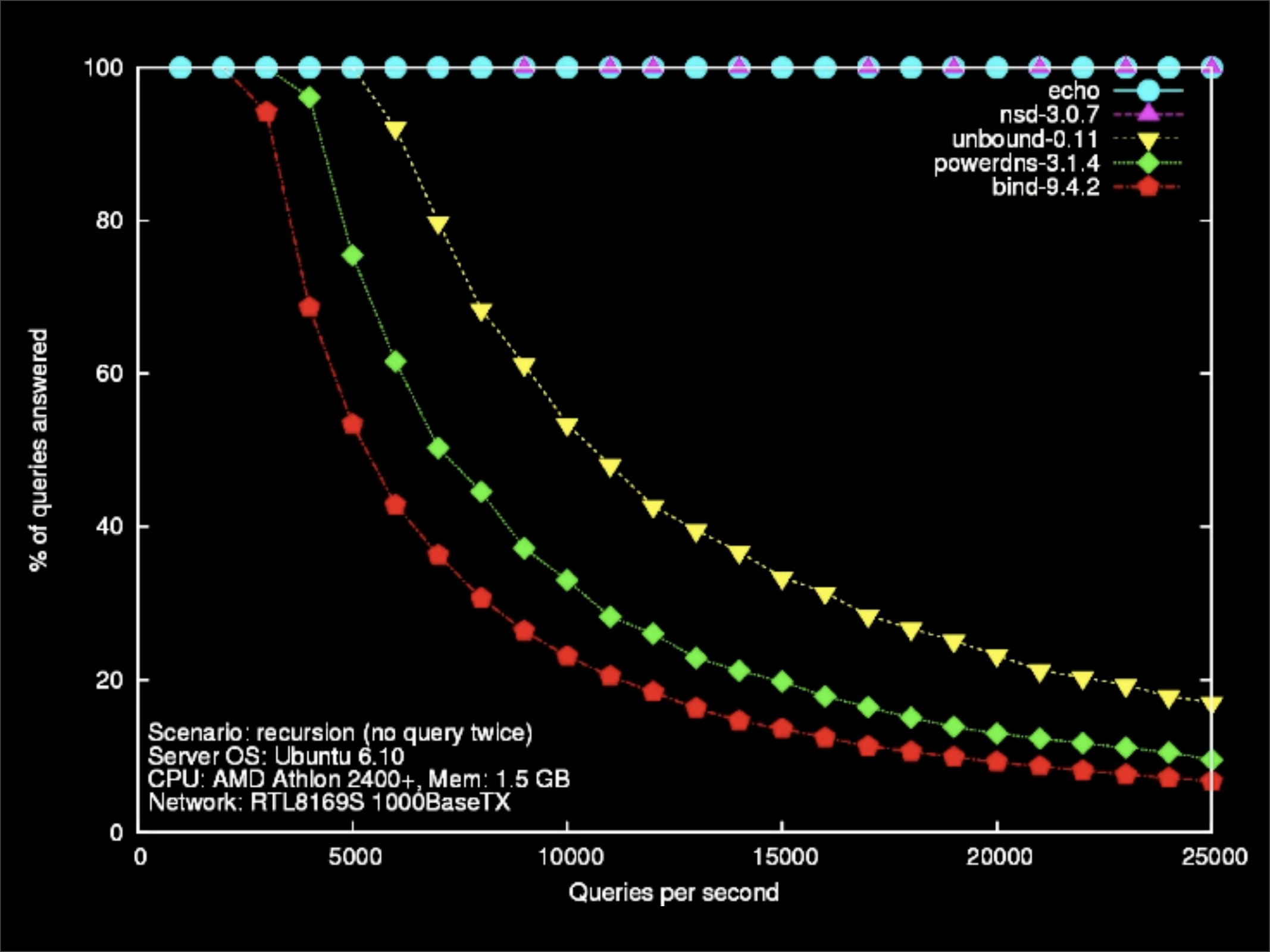
Security

- full implemented Forgery Resilience
  - qname matching
  - strong prng for ID/UDP/source address
  - RTT banding
- rfc 2181 trust model

Tests

- Regression Tests
- Beta Tests
- Performance Tests


100
80
60
40
20
0
% of queries answered
0
20000
40000
60000
80000
100000
120000
echo
nsd-3.0.7
unbound-0.11
powerdns-3.1.4
bind-9.4.2
Scenario: 100% cache response
Server OS: Ubuntu 6.10
CPU: AMD Athlon 2400+, Mem: 1.5 GB
Network: RTL8169S 1000BaseTX


100
80
60
40
20
0
% of queries answered
0
5000
10000
15000
20000
25000
Queries per second
echo
nsd-3.0.7
unbound-0.11
powerdns-3.1.4
bind-9.4.2
Scenario: recursion (no query twice)
Server OS: Ubuntu 6.10
CPU: AMD Athlon 2400+, Mem: 1.5 GB
Network: RTL8169S 1000BaseTX

Summary

- Unbound, validating caching resolver
- BSD license
- standards compliant, including DNSSEC
- High Performance
- runs on Linux, *BSD, Solaris, MacOS/X

Questions?

- unbound.net