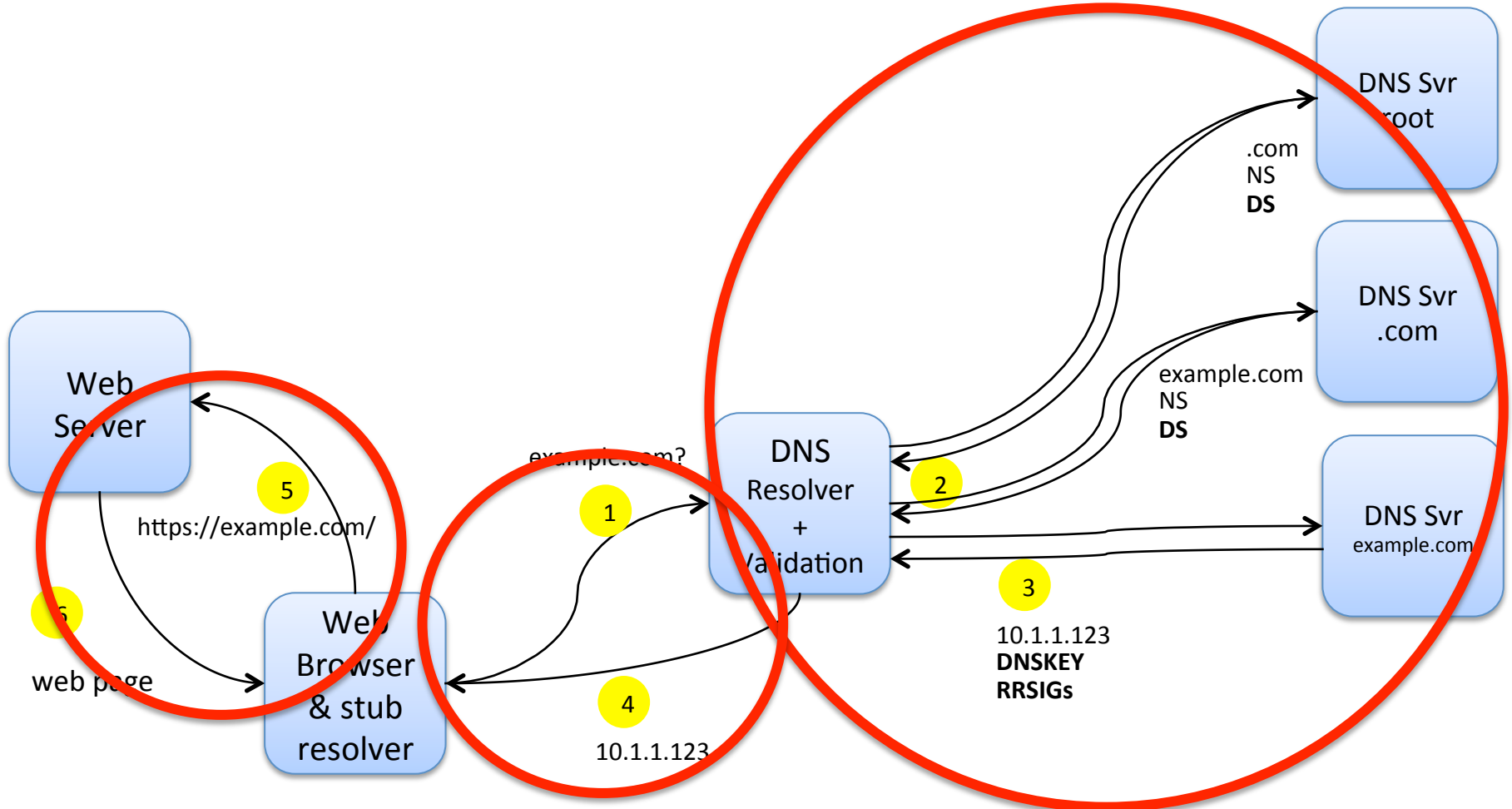


DNS / DNSSEC / DANE / DPRIVE Results at IETF 93 Hackathon

18-19 July 2015

Prague, Czech Republic

Summary – What We Are Working On



TRUST IN TLS - DANE

CONFIDENTIALITY - DPRIVE

INTEGRITY - DNSSEC

DNS at #IETFHackathon at #IETF93

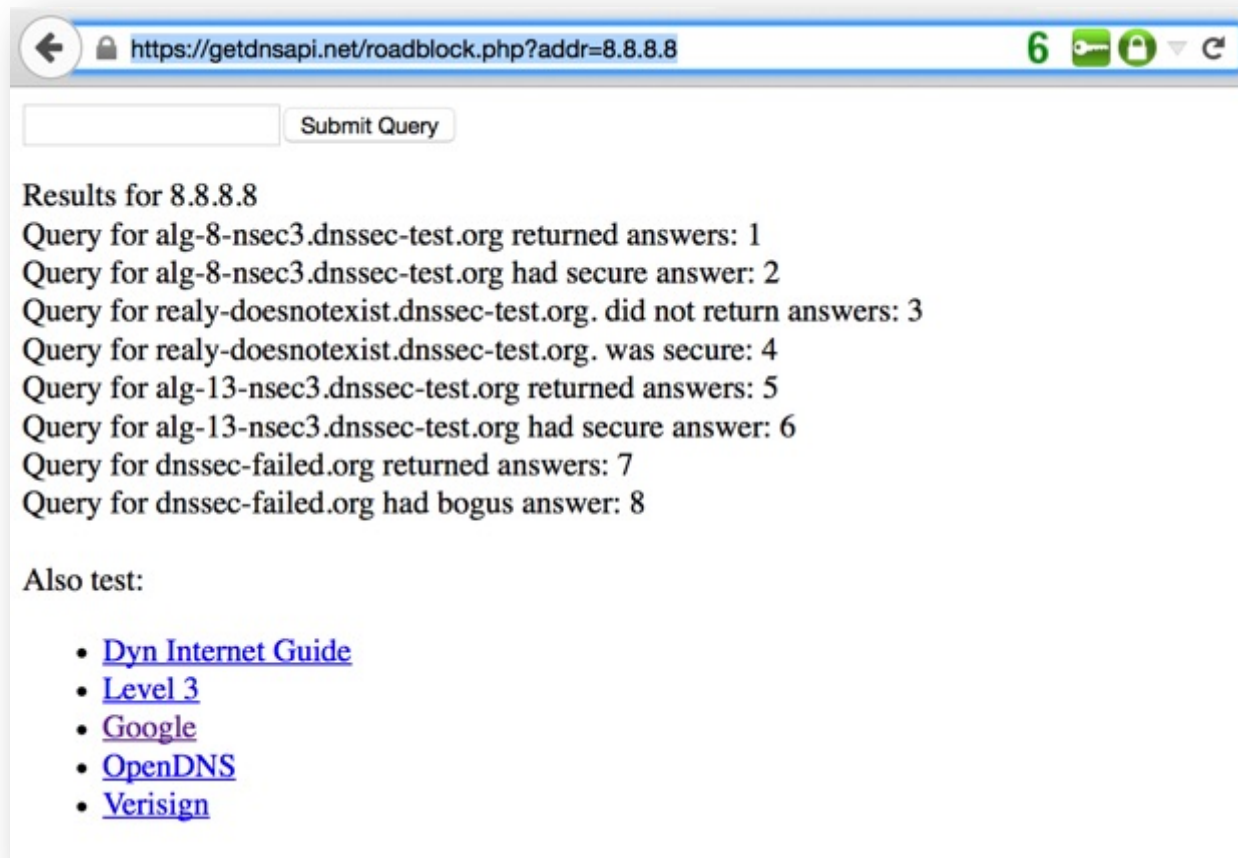
- **Visual interface to show what DNSSEC algorithms are supported by a DNS resolver**
- **Tool to test for DNSSEC roadblocks**
 - draft-ietf-dnsop-dnssec-roadblock-avoidance
- **Prototype web server implementation – TLS extension to deliver DNSSEC authentication chain to client**
 - draft-shore-tls-dnssec-chain-extension
- **DNS confidentiality/privacy (DPRIVE)**
 - Fixed opportunistic TLS in both getdns and Unbound to be strict authenticated TLS
 1. Added functionality to getdns API to authenticate TLS server.
 2. Patched Unbound server: forward-secret key exchange; enabled sending full TLS certificate chain in handshake
- **JSON interface to IANA registry of DNSSEC algorithms**

Public releases

- Visual interface to check DNSSEC algorithms
 - https://github.com/ogud/DNSSEC_ALG_Check
 - <https://github.com/getdnsapi/IETF93HackathonNode>
- Tool to test for DNSSEC roadblock avoidance
 - <https://www.ietf.org/registration/MeetingWiki/wiki/dnsresolvercapabilities>
 - <https://getdnsapi.net/roadblock.php>
 - <https://github.com/getdnsapi/IETF93HackathonPHP>
- DNS confidentiality/privacy - TLS
 - Patches going into next release of getdns API
 - Patch available for Unbound
- JSON interface to IANA registry of DNSSEC algorithms
 - <https://github.com/danyork/dnssec-algs-json>

Tool to test DNSSEC Roadblocks

- Implemented in PHP using getdns API



DNS Hackers

- Sara Dickinson
- Daniel Kahn Gillmor (dkg)
- Ólafur Guðmundsson
- Shumon Huque
- Allison Mankin
- Benno Overeinder
- Wendy Seltzer
- Willem Toorop
- Gowri Visweswaran
- Tim Wicinski
- Dan York