DNS / DNSSEC / DANE / DPRIVE @ IETF 93 Hackathon

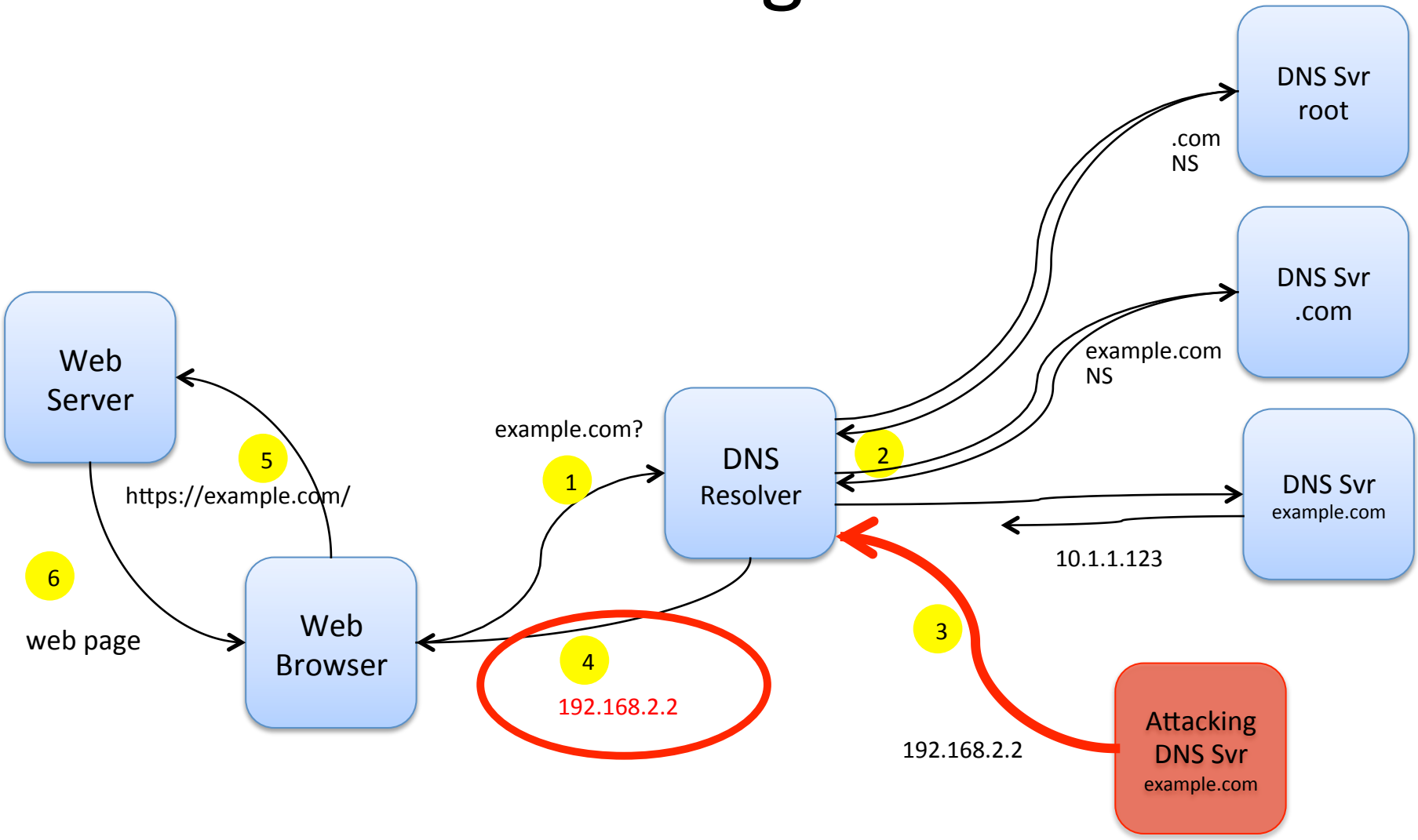
July 18-19
Prague, Czech Republic

https://www.flickr.com/photos/chrissam42/3989126075/

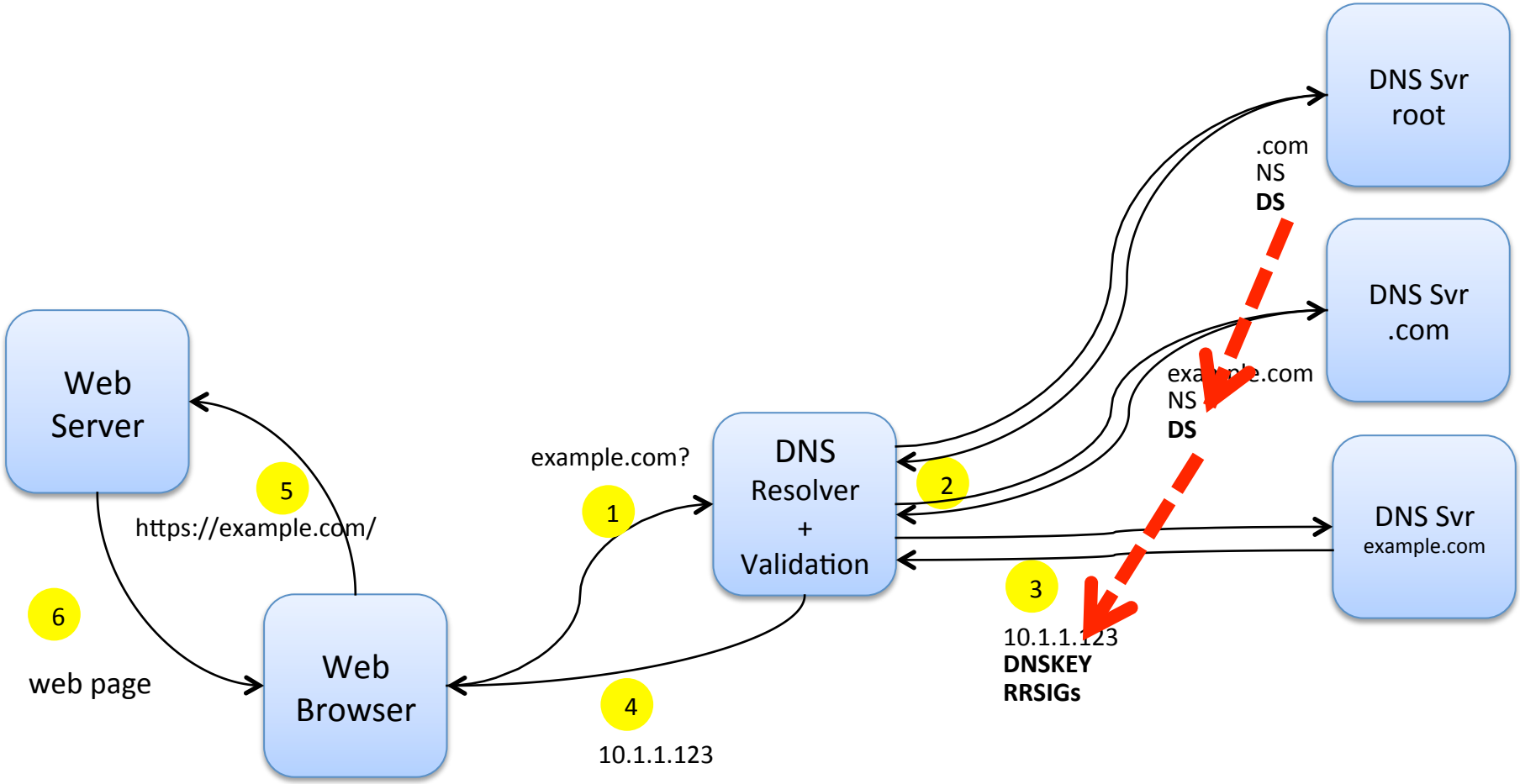
Answering 3 Questions

- **How can you be sure the information you get *out* of DNS is the same info the domain operator put *in* to DNS?** (DNSSEC)
- **How do you know you are using the correct TLS certificate?** (DANE/DNSSEC)
- **How can you protect the *confidentiality* of your DNS queries from surveillance?** (DPRIVE)

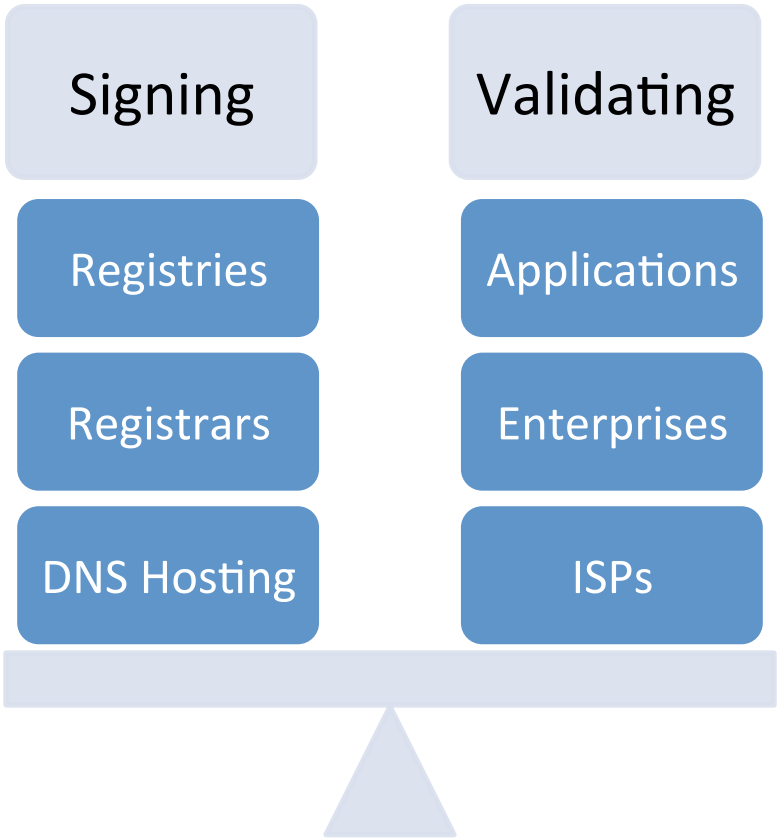
Attacking DNS



The Global Chain of Trust



The Two Parts of DNSSEC



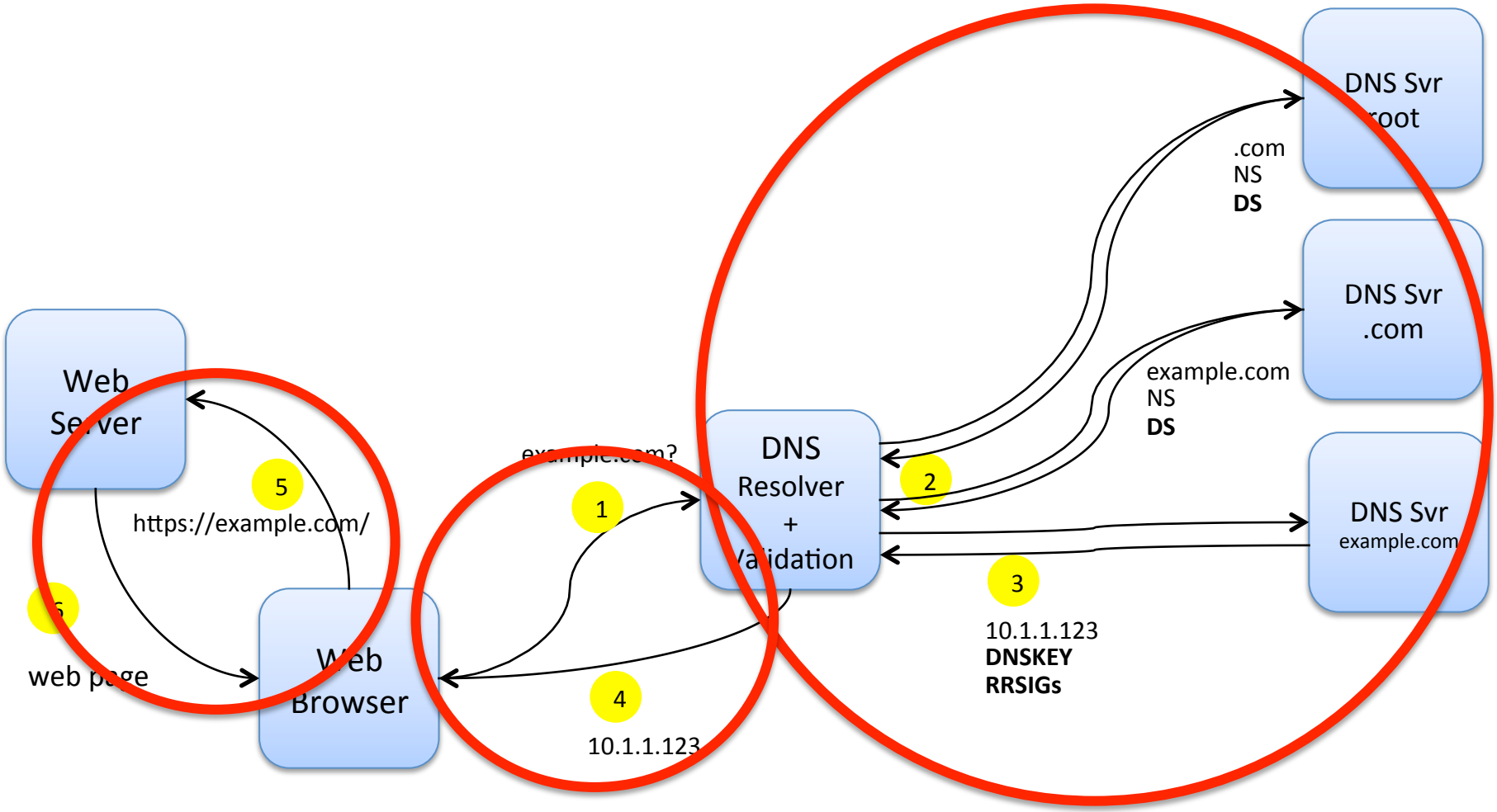
DANE

- RFC 6698
- Adds TLS certificate (fingerprint or entire cert) as a DNS record – and signs that with DNSSEC
- Apps can then verify via DNSSEC that this is correct cert (or CA) to use
- Being used now between email servers, XMPP servers, plugins for browsers
- Concept expanded to S/MIME certs, OpenPGP

DNS PRIVate Exchange (DPRIVE)

- Protecting the **confidentiality** of DNS queries
- https://datatracker.ietf.org/wg/dprive/charter/
- Focused on communication between DNS clients (i.e. stub resolvers) and DNS iterative resolvers
- Solutions include sending DNS queries over TLS or DTLS

Summary – What We Are Working On



TRUST IN TLS - DANE **CONFIDENTIALITY - DPRIVE** **INTEGRITY – DNSSEC**

IETF 93 Hackathon Ideas

- DNSSEC
  - Stats and reliability testing – improving tools to help gather data about roadblock avoidance.
  - Tools to help ease / automate deployment
  - Support for new algorithm types (ex. ECDSA) in tools/interfaces
- DANE
  - Portable tool for creating and adding DANE RR's to zones
  - Measurement of DANE deployment
  - Adding DANE support to different tools and interfaces
- DPRIVE
  - Explore mechanisms to authenticate server certificates used in DNS-over-TLS (Unbound, getdns)
  - Enhancements to the implementation of DNS-over-TLS in Unbound e.g.
    - TCP connection re-use/TLS session resumption
    - Configuration options for TLS versions and supported cipher suites
    - Transport fallback if TLS/STARTTLS not available

Join Us!

- **Help us make DNS (and the Internet) more secure and private!**

- Champions:
  - Dan York, Internet Society york@isoc.org
  - Allison Mankin, Verisign Labs amankin@verisign.com
  - Benno Overeinder, NLnet Labs benno@nlnetlabs.nl
  - Sara Dickinson, Sinodun sara@sinodun.com
  - Daniel Kahn Gillmor, ACLU dkg@fifthhorseman.net