



**OST**

Eastern Switzerland  
University of Applied Sciences

# Distributed Systems Advanced & Blockchain

**In the News**

Thomas Bocek

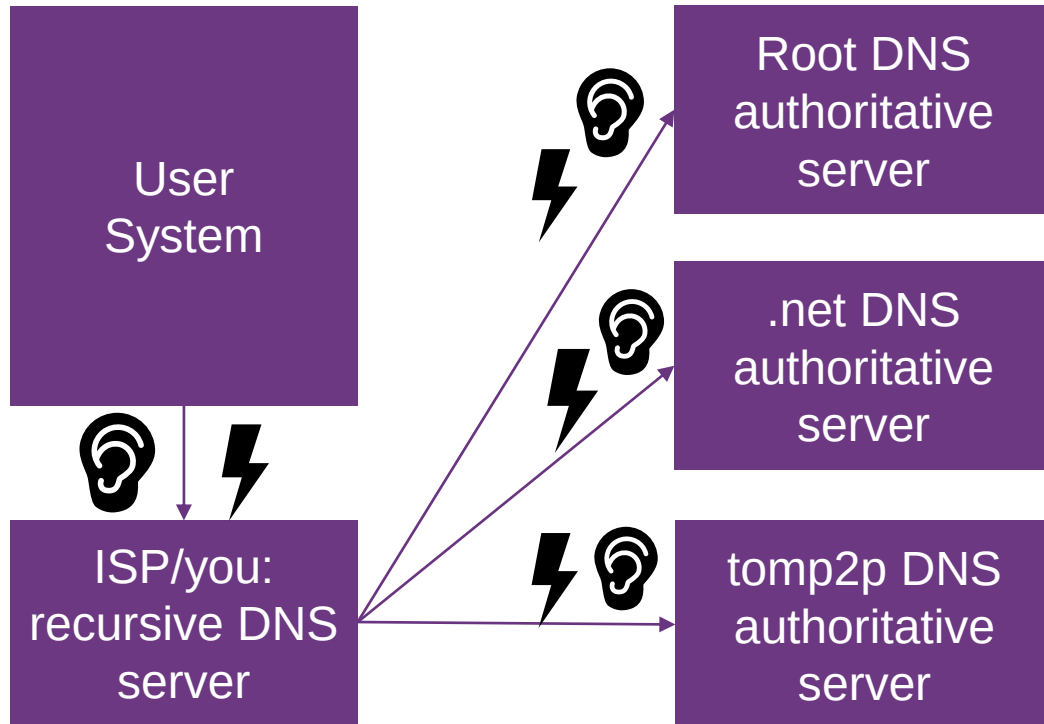
11 October 2020

# In the News

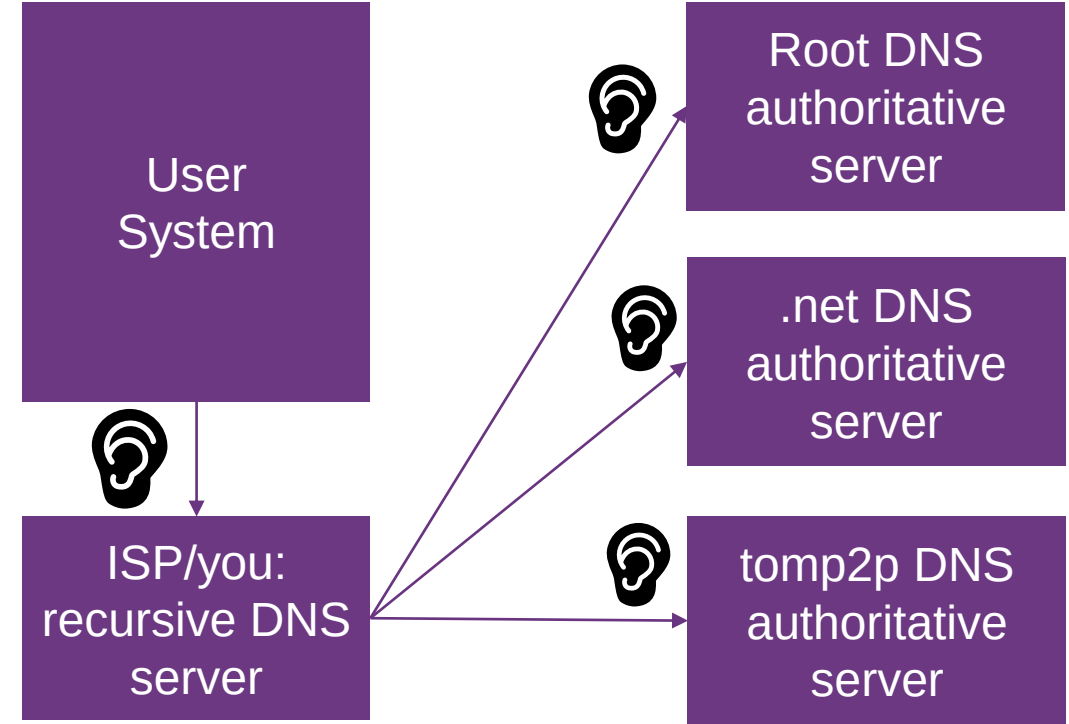
- 23.06.2020: [Interview with Dr. Paul Mockapetris](#), creator of DNS
  - History: hosts.txt maintained by Stanford
  - DNS: dsl.hsr.ch → Java Package ch.hsr.dsl
    - “I designed it this way for autocomplete... Imagine if we were to type “com.” and then wait for autocomplete. Out of 160 million choices, there would be a pretty long pull-down menu.”
  - DoH (DNS over HTTPS)
    - “But suppose that DNSSEC does give you security—I’m not sure whether all of my DNS to Google or Cloudflare DNS servers [which perform DNSSEC by default] is what I really want if I’m interested in preserving my privacy.”
- 25.02.2020: [The Facts: Mozilla’s DNS over HTTPs \(DoH\)](#)
  - DNS is unencrypted → DNSSEC signs but does not encrypt
    - DNS over TLS (DoT) vs. DNS over HTTPS (DoH)
  - Mozilla: “Today in practice, DNS is centralized because consumer devices are locked to the DNS service of ISPs”
  - Very controversial topic:
    - Argument: 5 ISPs per country, this is centralized, DoH with cloudflare is less centralized?
    - Application manages DNS, different result for different applications, but possible to query DNS from Javascript
    - <https://ungleich.ch/en-us/cms/blog/2019/09/11/turn-off-doh-firefox/>
    - [Google](#): wont override choice of DNS provider

# Application Protocol: DNS

- DNS

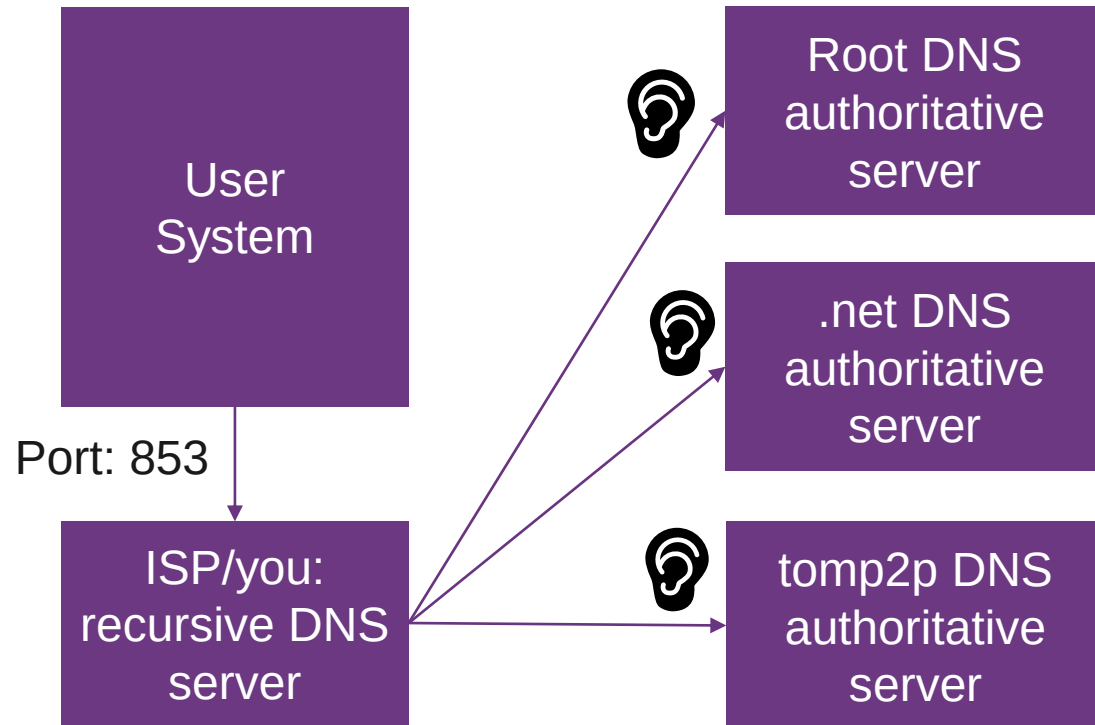


- DNSSEC

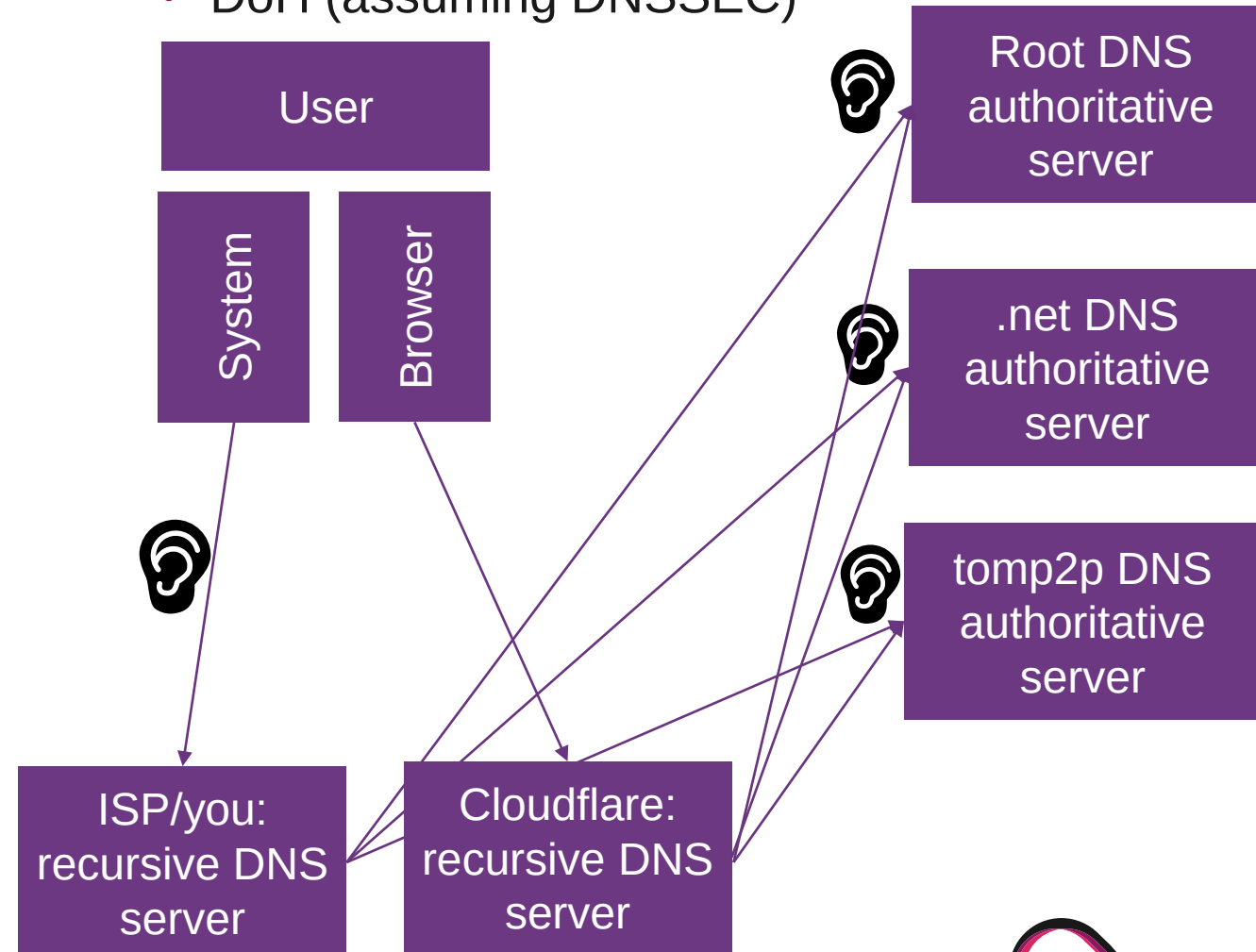


# Application Protocol: DNS

- DoT (assuming DNSSEC)



- DoH (assuming DNSSEC)



# The DNS war

## DoH

- provides confidentiality of lookups in transit
- Uses standard HTTP/2, on the standard port (443)
  - Cannot distinguish between traffic/DNS
- Trivially deployed, DNS responses are served like simple web pages
- Performance: TCP+TLS handshake → 2/3 RTT
  - But: Cloudflare is close to you
- Difficult upgrade path for clients: per-application installation
- Browsers can perform DNS queries using Javascript

## DoT

- provides confidentiality of lookups in transit
- DNS over TLS, separate port (853)
  - Can be blocked
- Widely supported by serving software (Bind, PowerDNS, Unbound) and public resolvers (Cloudflare, Quad9, Google)
- Performance: TCP+TLS handshake → 2/3 RTT
  - But: ISP is close to you
- Easy upgrade path for clients: clients can test if the configured resolver supports DoT on port 853, fall back to DoU53 otherwise)



# In the News

- 23.06.2020: [Interview with Dr. Paul Mockapetris](#), creator of DNS
  - “Do you think we could use blockchain with DNS?”
  - “I think we could use distributed ledger technologies for the operation of registries and registrars.”
  - “I once proposed to the ICANN people that they could just have the root managed by a voting system of the existing TLDs and you could have them vote on whether to admit new TLDs. You could think about having algorithms that are implemented using ledger technology to automate some of the bureaucratic functions here.”
- 07.10.2020: [How The URL Was Built](#)
  - [Tim Berners-Lee](#): “I have to say that now I regret that the syntax is so clumsy. I would like `http://www.example.com/foo/bar/baz` to be just written `http:com/example/foo/bar/baz` where the client would figure out that `www.example.com` existed and was the server to contact.”
- 07.10.2020: [Chrome is deploying HTTP/3 and IETF QUIC](#)
  - “responsible for carrying over a third of Google traffic”
  - “Google search latency decreases by over 2%. YouTube rebuffer time decreased by over 9%, while client throughput increased by over 3% on desktop and over 7% on mobile”