deSEC, DNSSEC & Friends

DDI User Group
December 2, 2021

Dr. Peter Thomassen
peter.thomassen@securesystems.de

SSE

peter:~$ whoami

- Historically, a particle physicist (Ph.D. 2016)
    - Big data analysis at the CERN Large Hadron Collider (LHC)
- Working for **Secure Systems Engineering** (Berlin)
    - **IT security** for various industries (media & tech, financial, health, public/gov)
    - Both **defensive** (plan, implement, audit/review) and **offensive** (penetration testing)
- Long-term interest in Internet Security
    - 20 years experience in running Internet services
    - Started deSEC in 2014 to “fill the DNSSEC gap”
- Otherwise, passionate choir singer :-)

Overview

- **deSEC**
  - **What is it?**
  - **Example: Public Suffix List DNS Query Service**

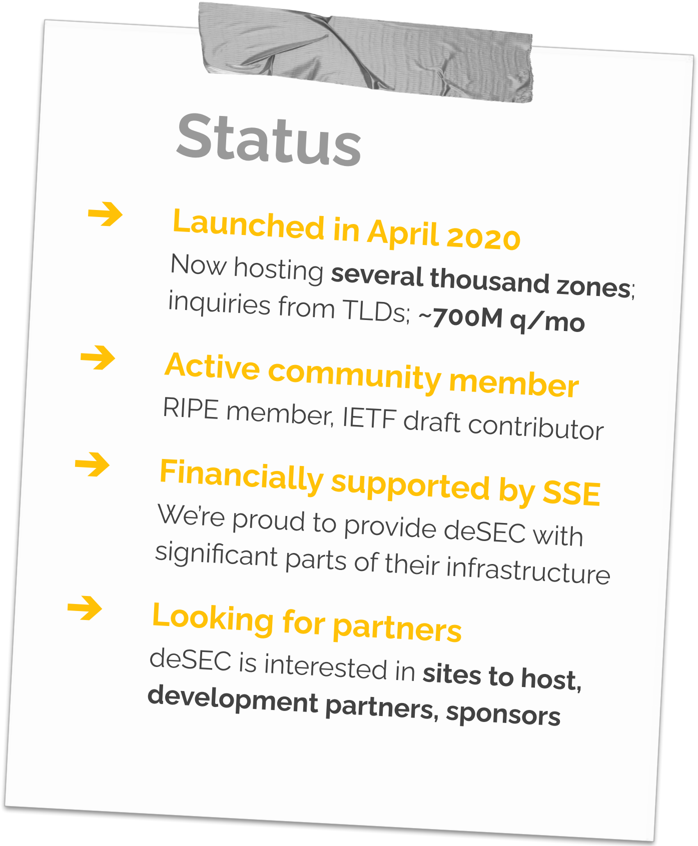
- DNSSEC
  - Introduction
  - State of DNSSEC
  - Don’t be afraid!

- Advanced DNSSEC Topics
  - DNSSEC Bootstrapping
  - (Multisigner)

A free DNS hosting service, designed with security in mind.

deSEC is a **non-profit** doing the same thing as **Let's Encrypt, but for DNSSEC**.

- all **automatic** DNSSEC
- **fancy API** and GUI
- support for modern stuff (e.g. DANE)
- **dynDNS** service (under dedyn.io)



Status

→ **Launched in April 2020**
Now hosting **several thousand zones**; inquiries from TLDs; **~700M q/mo**

→ **Active community member**
RIPE member, IETF draft contributor

→ **Financially supported by SSE**
We're proud to provide deSEC with significant parts of their infrastructure

→ **Looking for partners**
deSEC is interested in **sites to host, development partners, sponsors**

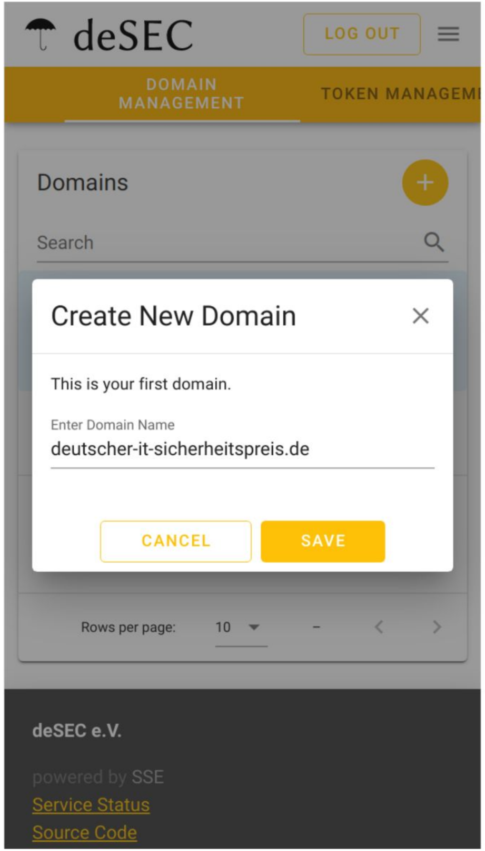
Using deSEC 101

GUI

- **Straightforward**
- Reactive
- **Field-level validation**
- Mobile-friendly
- Zero external resources

REST API (https://desec.readthedocs.io/)

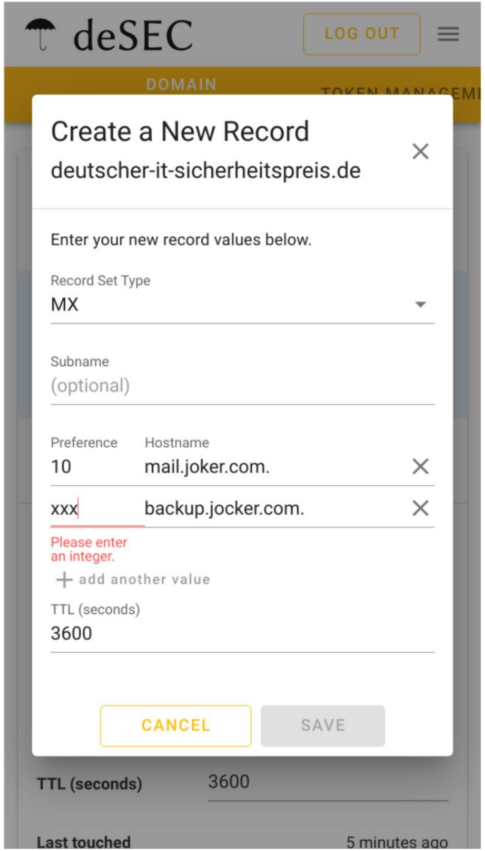
- Helpful **validation**
- **Transactional** bulk actions
- Paging, API token scoping, …



Create New Domain

This is your first domain.

Enter Domain Name: deutscher-it-sicherheitspreis.de



Create a New Record
deutscher-it-sicherheitspreis.de

Enter your new record values below.

Record Set Type: MX

Subname: (optional)

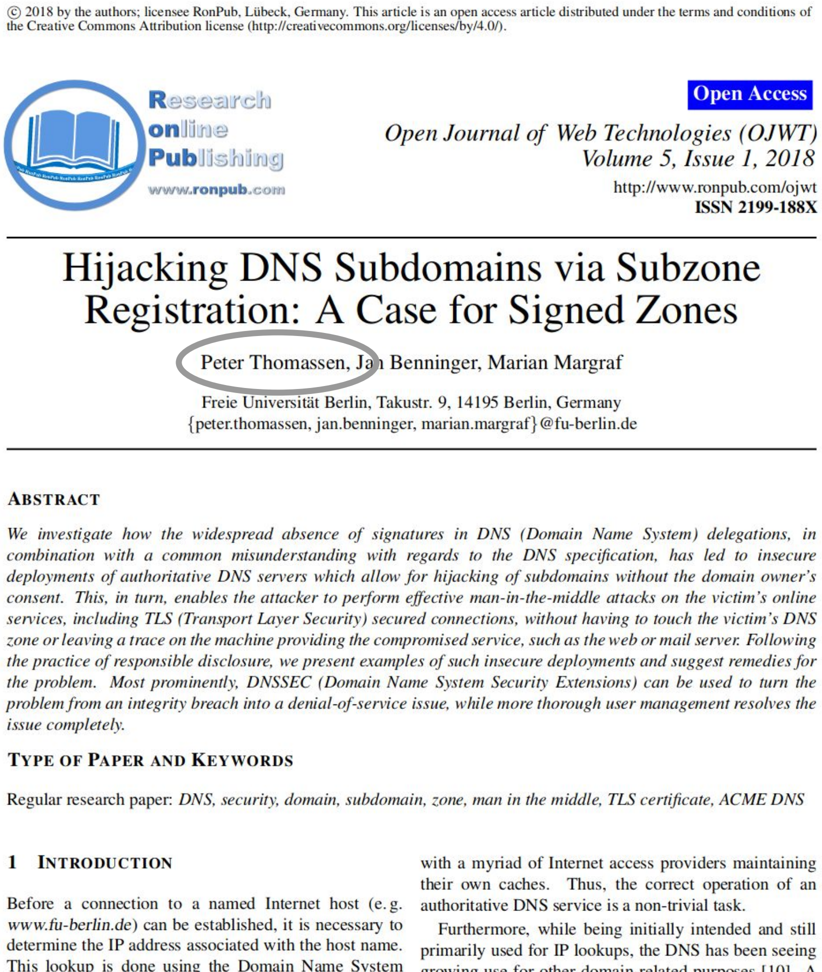
Preference	Hostname
10	mail.joker.com.
xxx	backup.jocker.com.

Please enter an integer.

TTL (seconds): 3600

TTL (seconds) 3600

Last touched 5 minutes ago



© 2018 by the authors; licensee RonPub, Lübeck, Germany. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).

Research online Publishing
www.ronpub.com

Open Access

Open Journal of Web Technologies (OJWT)
Volume 5, Issue 1, 2018
http://www.ronpub.com/ojwt
ISSN 2199-188X

Hijacking DNS Subdomains via Subzone Registration: A Case for Signed Zones

Peter Thomassen, Jan Benninger, Marian Margraf

Freie Universität Berlin, Takustr. 9, 14195 Berlin, Germany
{peter.thomassen, jan.benninger, marian.margraf}@fu-berlin.de

ABSTRACT

We investigate how the widespread absence of signatures in DNS (Domain Name System) delegations, in combination with a common misunderstanding with regards to the DNS specification, has led to insecure deployments of authoritative DNS servers which allow for hijacking of subdomains without the domain owner's consent. This, in turn, enables the attacker to perform effective man-in-the-middle attacks on the victim's online services, including TLS (Transport Layer Security) secured connections, without having to touch the victim's DNS zone or leaving a trace on the machine providing the compromised service, such as the web or mail server. Following the practice of responsible disclosure, we present examples of such insecure deployments and suggest remedies for the problem. Most prominently, DNSSEC (Domain Name System Security Extensions) can be used to turn the problem from an integrity breach into a denial-of-service issue, while more thorough user management resolves the issue completely.

TYPE OF PAPER AND KEYWORDS

Regular research paper: *DNS, security, domain, subdomain, zone, man in the middle, TLS certificate, ACME DNS*

1 INTRODUCTION

Before a connection to a named Internet host (e. g. *www.fu-berlin.de*) can be established, it is necessary to determine the IP address associated with the host name. This lookup is done using the Domain Name System

with a myriad of Internet access providers maintaining their own caches. Thus, the correct operation of an authoritative DNS service is a non-trivial task.

Furthermore, while being initially intended and still primarily used for IP lookups, the DNS has been seeing growing use for other domain related purposes [10]. A

- While building deSEC, we identified a few security pitfalls
- Some providers apparently didn't
- We managed to take over DNS zones and issue Let's Encrypt certificates at affected providers
- Responsible disclosure, then scientific write-up + publication

Building on top of deSEC

The Public Suffix List (PSL)

> *A "public suffix" is one under which Internet users can (or historically could) directly register names. Some examples of public suffixes are `.com`, `.co.uk` and `pvt.k12.ma.us`. The Public Suffix List is a list of all known public suffixes.*
>
> — https://publicsuffix.org/

What does that mean?

- Informs about organization and policy boundaries in the domain space
- Supports wildcards, and exceptions from wildcards
- Maintained by the community (on GitHub) and provided as a text file

PSL in the Real World

Use Cases

- Browsers
- Certificate issuance (think of `*.co.uk`)
- Multi-tenant DNS operation ← our motivation (DNS platform desec.io)
- DMARC

Practical Considerations

- Applications have to **bring a copy** of the list, and need to **keep it up to date**
- Parsing & extracting information from PSL requires **multi-staged algorithm** 😨

… enter our DNS-based PSL Query Service

Implemented PSL using the DNS **under `query.publicsuffix.zone`**

- No need for applications to parse or refresh the PSL altogether
- **Public suffix** can be retrieved ad-hoc **with a simple PTR lookup** (cacheable!)
  - No need for specialized tooling
- Hosted at deSEC → **DNSSEC ensures authenticity**

```
$ dig +noall +answer PTR www.honest-consulting.de.query.publicsuffix.zone
www.honest-consulting.de.query.publics… 21600 IN CNAME  de.query.publics…
de.query.publicsuffix.zone.              7199 IN PTR    de.
```

→ https://publicsuffix.zone/ has a **live demo**

Overview

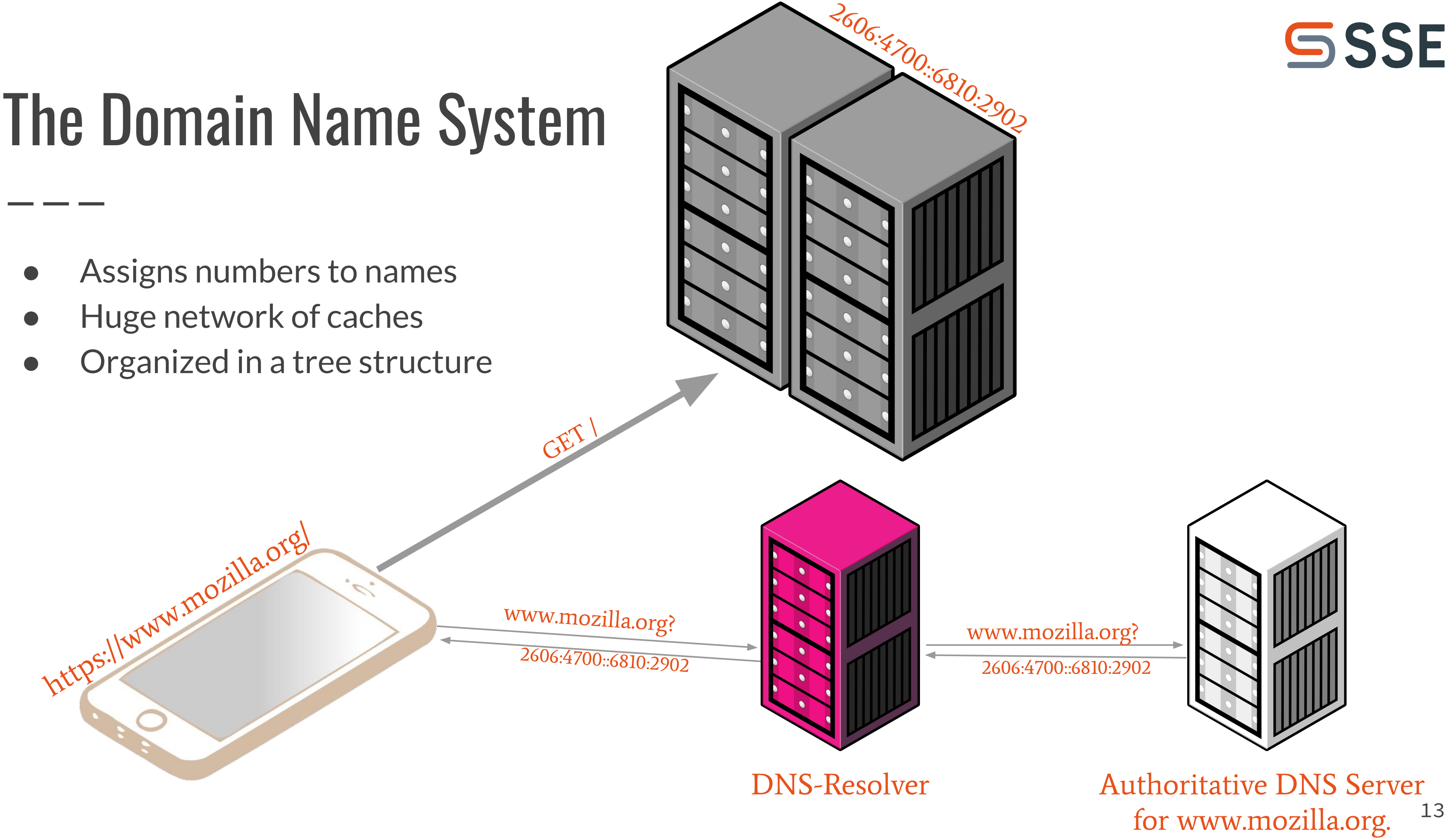
- deSEC
  - What is it?
  - Public Suffix List DNS Query Service

- **DNSSEC**
  - **Introduction**
  - **State of DNSSEC**
  - **Don’t be afraid!**

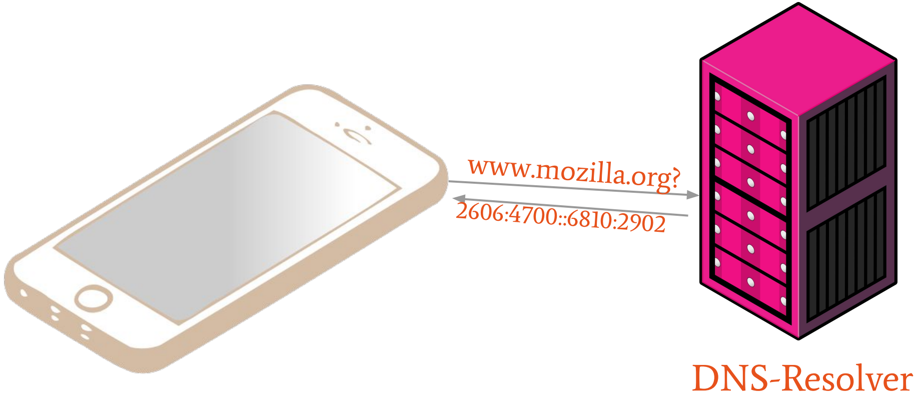
- Advanced DNSSEC Topics
  - DNSSEC Bootstrapping
  - (Multisigner)

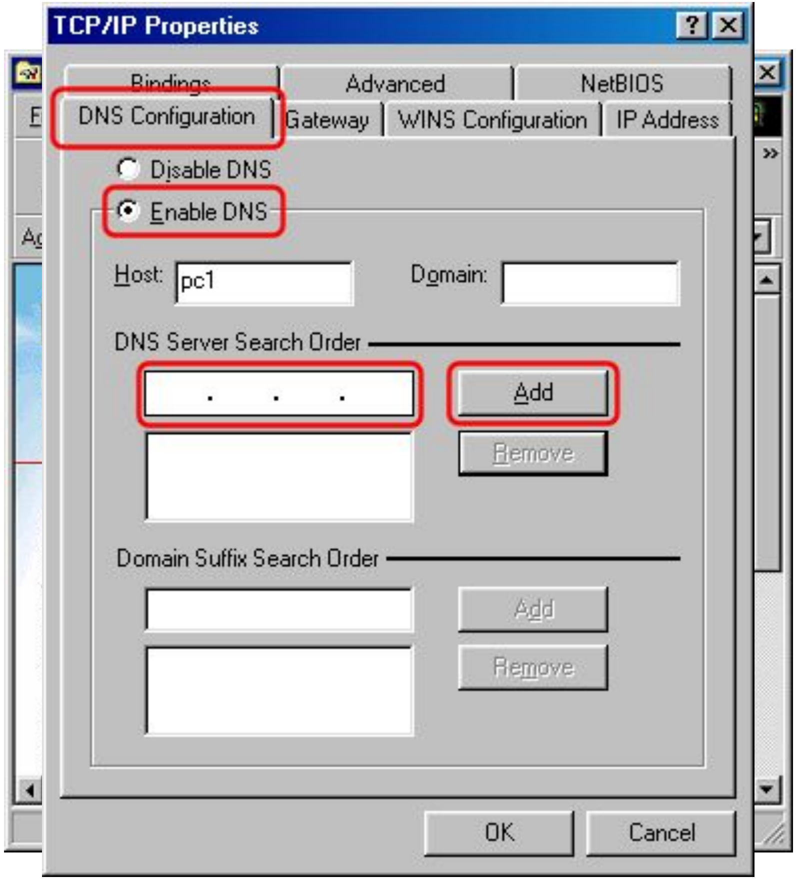
The Domain Name System

- Assigns numbers to names
- Huge network of caches
- Organized in a tree structure



Clients and DNS Resolvers




TCP/IP Properties

Bindings | Advanced | NetBIOS

DNS Configuration | Gateway | WINS Configuration | IP Address

○ Disable DNS

● Enable DNS

Host: pc1 Domain:

DNS Server Search Order

. . .

Add

Remove

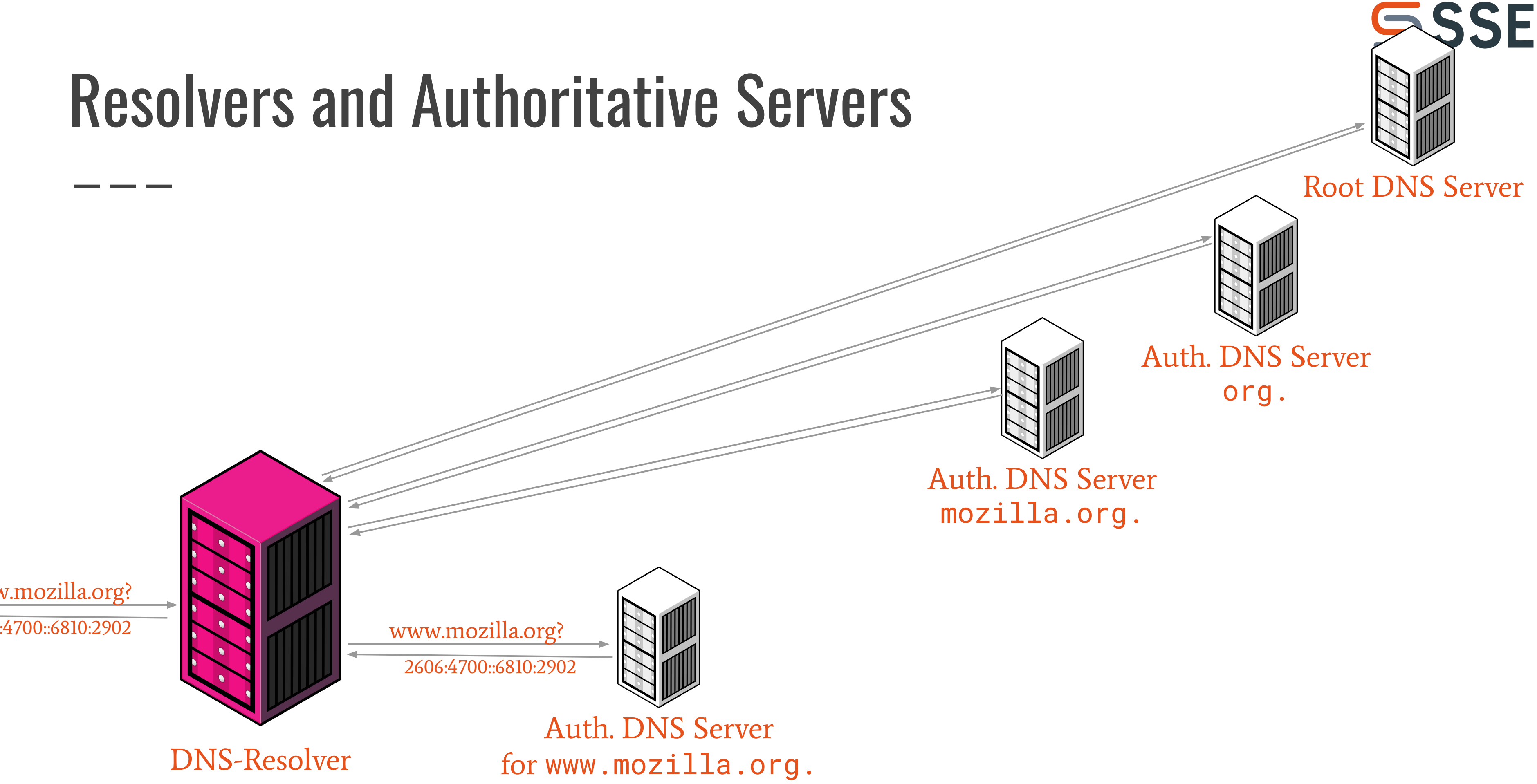
Domain Suffix Search Order

Add

Remove

OK Cancel

Resolvers and Authoritative Servers



Root DNS Server

Auth. DNS Server
`org.`

Auth. DNS Server
`mozilla.org.`

v.mozilla.org?

:4700::6810:2902

www.mozilla.org?

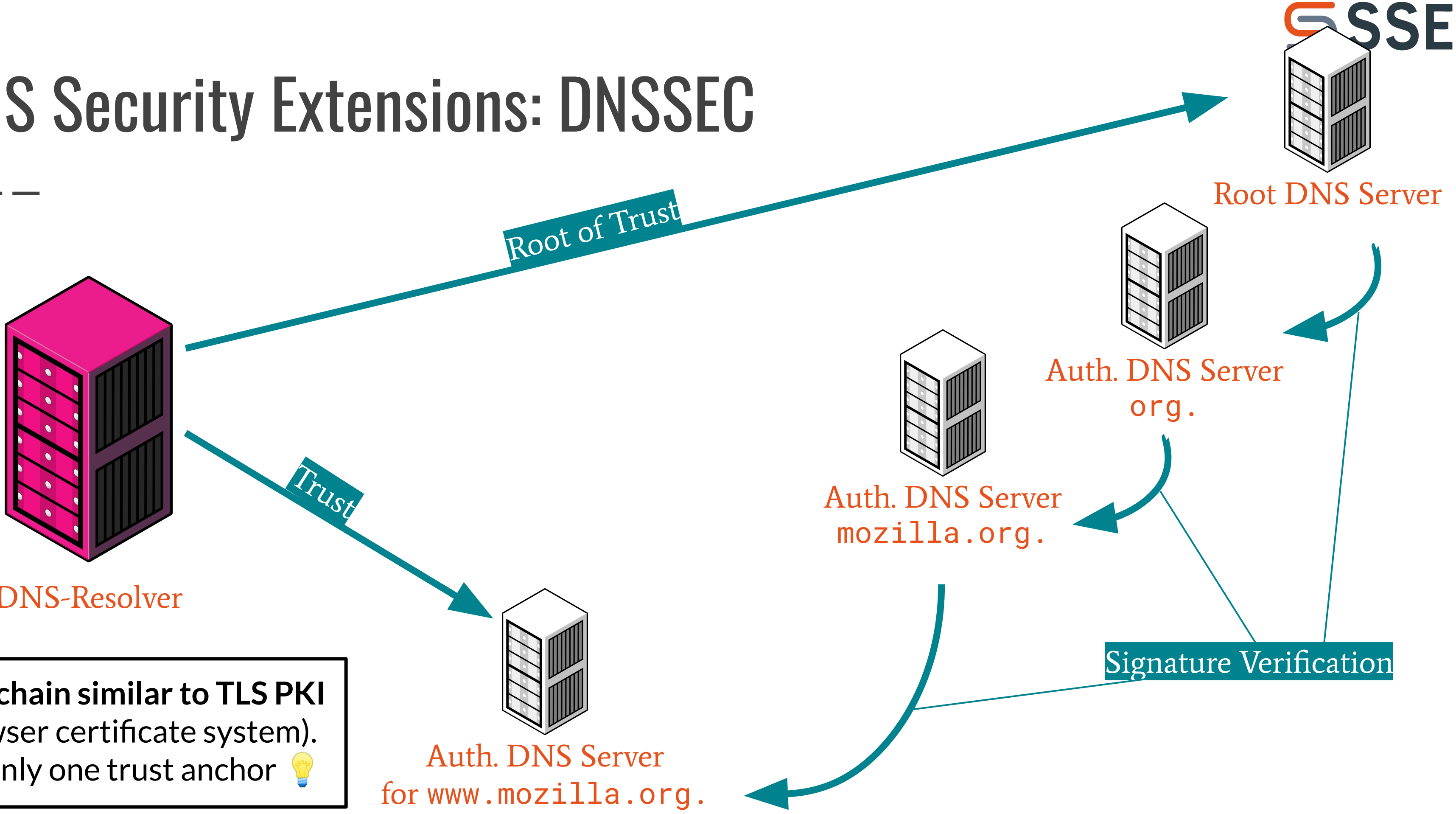
2606:4700::6810:2902

DNS-Resolver

Auth. DNS Server
for `www.mozilla.org.`

SSE

DNS Security Extensions: DNSSEC



Trust chain similar to TLS PKI
(browser certificate system).
But: only one trust anchor 💡

DNSSEC validation rate

28 %

- 28% globally
- 50–95% in some places

vs.

secure delegation rate

5 %

- 5% globally
- 50–70% in some places
- **even for signed zones: < 50%**

Sources: deSEC, https://stats.labs.apnic.net/dnssec, https://rick.eng.br/dnssecstat/, https://www.sidn.nl/en/news-and-blogs/dnssec-adoption-heavily-dependent-on-incentives-and-active-promotion

But why?!

Why is it so bad?

- Mostly: it is too **difficult to turn on DNSSEC**
  - You need to **get your public key data signed by the parent**
  - Most domain owners don't take care of this (don't even know!)

- DNS infrastructure emerges slowly
  - Availability is critical → **no experiments**
  - Visibility is low → **DNS is a cost center**, not a feature

- Some are **afraid of DNSSEC**
  - **Don't be afraid!**
  - DNSSEC enables **so many cool things**, like **key exchange** (TLSA etc.)

Don’t be afraid.

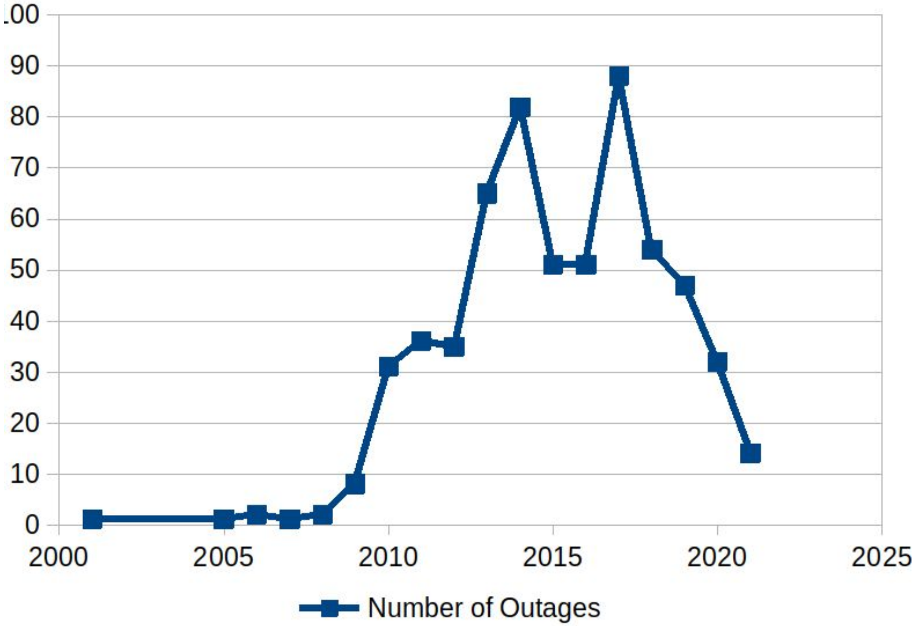
- Early days (> 5 years ago), **signing and key rollovers were manual processes**

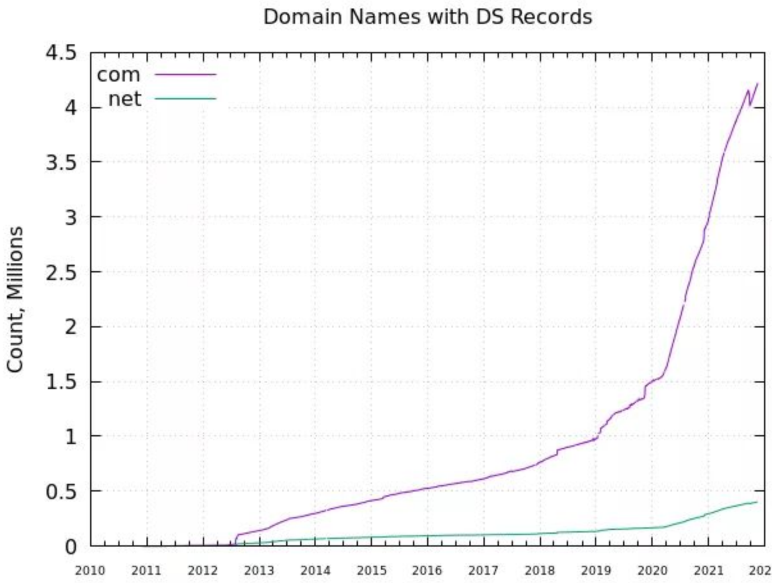
- **Today, there’s great tooling** out there
  - Knot DNS even can do key rollover (including waiting for cache expiry etc.)

- Number of **deployments growing**, number of **incidents shrinking**
  → **decreasing risk** per deployment

- Of course, some things still go wrong
  - Most recently, Amazon Route 53 messed up slack.com (https://slack.engineering/what-happened-during-slacks-dnssec-rollout/)

Don’t be afraid.





https://ianix.com/pub/dnssec-outages.html

https://scoreboard.verisignlabs.com/

Overview

- deSEC
    - What is it?

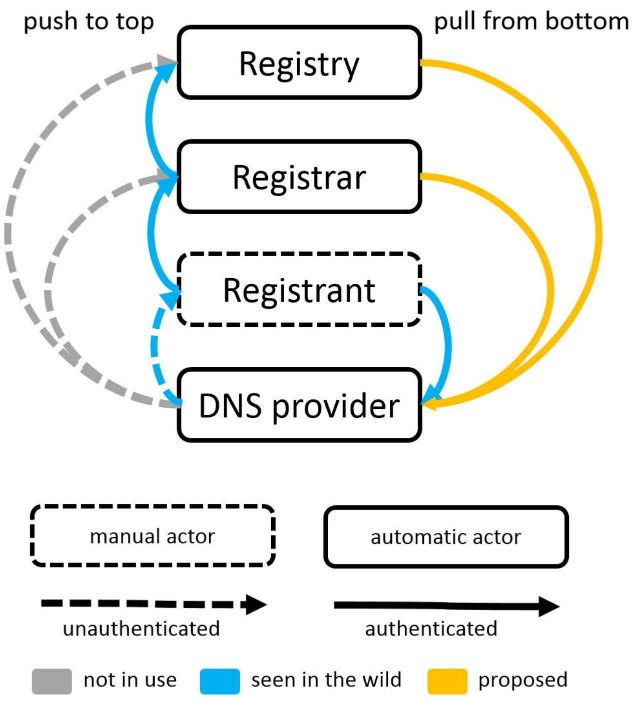
Nerd Alert

    - Introduction
    - State of DNSSEC
    - Don’t be afraid!

- **Advanced DNSSEC Topics**
    - **DNSSEC Bootstrapping**
    - (Multisigner)

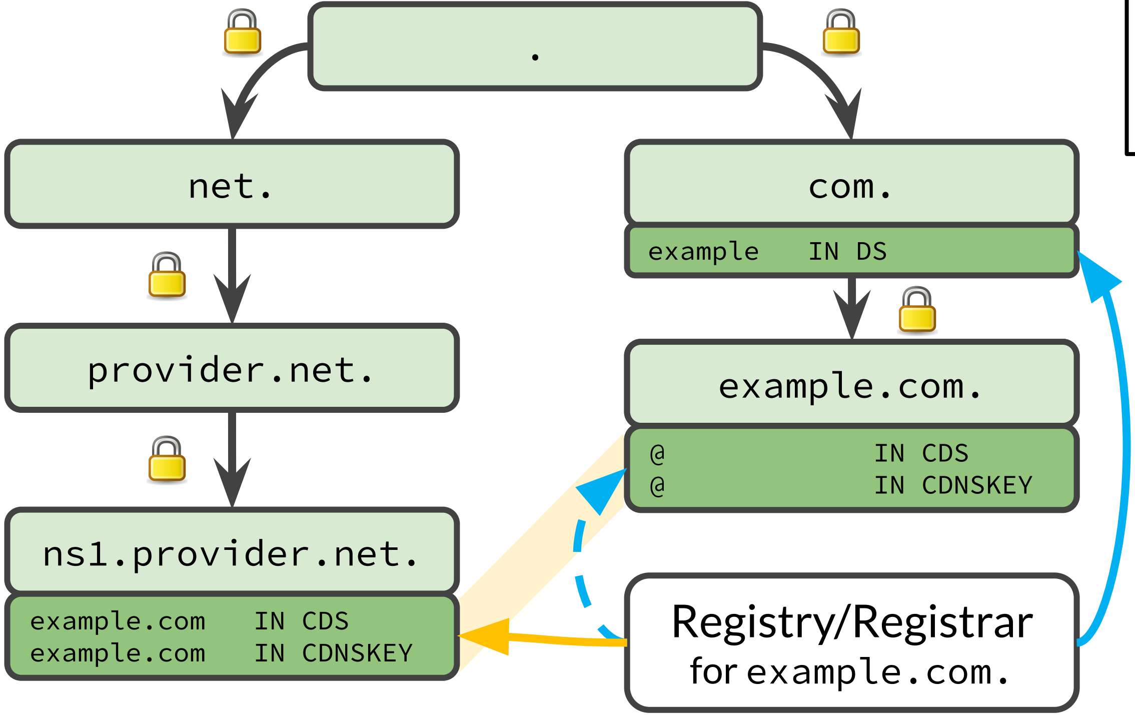
Approaches to DS Bootstrapping

- Various methods have emerged
  - TOFU, manual submission, REST interfaces*, CDS/CDNSKEY from insecure (RFC 8078)
- Each suffers from one or more downsides
  - unauthenticated || out of band || slow || stateful || error-prone || too many parties || no automation
  - **Authenticated workflow involves too many steps**
- **Goal: add authentication to direct pull** from DNS operator
  - **automatable, immediate, no state required**



[*] ICANN 54 (2015), draft-ietf-regext-dnsoperator-to-rrr-protocol (2018)

CDS Authentication: Co-Publish under Trusted Hostname



💡 Use an **established chain of trust** (left) to take a detour

- authenticated, immediate
- no active on-wire attacker

Status & Outlook

- Huge potential
  - e.g. Cloudflare could turn on DNSSEC for ~19% of Top 1M domains (Tranco dataset)

- We contributed this proposal to the IETF DNSOP Working Group
  - https://datatracker.ietf.org/doc/draft-thomassen-dnsop-dnssec-bootstrapping/

- Reactions have been positive
  - Document will likely become official IETF work item
  - Experimental implementations under way (e.g. GoDaddy)

- **Looking for DNS operators and registries/registrars** who are interested in deploying the protocol (as an experiment?)

Thank you!

Questions?

Backup

Recap: We got ...

Signaling

- of **zone-specific** information
- from the **NS operator**
- **to the public** (e.g. the parent)

... which is

- **authenticated,**
- **in-band,**
- **immediate,**
- requires **no third parties.**

Besides bootstrapping:

What else can be done with it?

Multisigner Key Exchange (in a Nutshell)

Multisigner Goals (RFC 8901):

- **Redundancy:** multi-homed zones with full validation of responses
- **Integrity:** smooth transition during provider transfer **(w/o going insecure)**

How it works:

- Operators **advertise each others' ZSKs** via the DNSKEY set that they sign;
- Parent **advertises all of the KSKs via its DS records**.

How can operators learn each other's ZSKs?

- Publish them in a DNSKEY RRset at `example.com.`*`ns1.other.net`*
- **Same signaling mechanism** as for DS bootstrapping