

Hackathon Results

Project ~~DNS~~ XoT

IETF 110
March 1-5, 2021
Online



IETF110 DNS Hackathon - Community OARC Mattermost

DNS-OARC +

IETF110 DNS Hackathon

System 12:02
@willem updated the channel display name from: IETF109 Hackathon to: IETF110 DNS Hackathon

habbie 12:02
I feel moved
👍 1

System 12:03
@willem updated the channel header
From: Enter your projects here:
<https://trac.ietf.org/trac/ietf/meeting/wiki/109hackathon>
To: Enter your projects here:
<https://trac.ietf.org/trac/ietf/meeting/wiki/110hackathon>

shane 12:08
Is there any interest in doing a "pre-COVID" style hackathon, where we take a weekend and hack then, instead of a "hackthon" which spreads over a week and doesn't involve people actually getting together in any meaningful way?

vcunat 12:09
I had actually wondered why this changed instead of just making it online.

habbie 12:09
my 2 cents: a hackathon week will see me doing 3 small 15 minute things over that week. A hackathon weekend will see me putting in several hours, or absolutely nothing.

habbie

Write to IETF110 DNS Hackathon

thon Plan for DNS

IETF110 DNS Hackathon - Community OARC Mattermost

DNS-OARC

IETF110 DNS Hackathon

System 12:02
@willem updated the channel display name from: IETF109 Hackathon to: IETF110 DNS Hackathon

habbie 12:02
I feel moved
👍 1

System 12:03
@willem updated the channel header
From: Enter your projects here:
<https://trac.ietf.org/trac/ietf/meeting/wiki/109hackathon>
To: Enter your projects here:
<https://trac.ietf.org/trac/ietf/meeting/wiki/110hackathon>

shane 12:08
Is there any interest in doing a "pre-COVID" style hackathon, where we take a weekend and hack then, instead of a "hackthon" which spreads over a week and doesn't involve people actually getting together in any meaningful way?

vcunat 12:09
I had actually wondered why this changed instead of just making it online.

habbie 12:09
my 2 cents: a hackathon week will see me doing 3 small 15 minute things over that week. A hackathon weekend will see me putting in several hours, or absolutely nothing.

habbie

Write to IETF110 DNS Hackathon

IETF110 DNS Hackathon - Community OARC Mattermost

DNS-OARC

IETF110 DNS Hackathon

willem 14:47
@shane How about an in-person hackathon "weekend" or "Saturday" at the NLnet Labs office. Either prior or right after the official IETF hackathon week? I'll try to arrange beer and proper lunches and dinner with @benno for the occasion. The other Dutchies could join too @habbie @matthijs?
(edited)

System 14:47
@matthijs added to the channel by you.

habbie 14:48
Commented on willem's message: @shane How about an in-person hackathon "w...
Not until we're all vaccinated..

habbie 14:48
(As good as that sounds, though! 😊)

vcunat 14:58
Reminded me that IETF 111 page sounds like it might be in-person, but it seems very unlikely I could get vaccinated by July. (Honestly I'm not really sure I can get even by 112.)

matthijs 15:05
I am interested as long as I can come by car (no public transport), we can maintain social distance, and the place is well ventilated. It also depends on what Covid-19 regulations we have next month.

willem 15:30
@matthijs you know the place, though we have now more spaces than before. We now have almost all of the spaces of the right wing on the ground floor. I'll make sure all windows are open.
(edited)

matthijs 15:33
I'll bring a jacket 😊

willem 15:34
Yay!

Write to IETF110 DNS Hackathon

NS

Hackathon Plan for DNS - Sat 6th March



Hackathon Plan

The **Xot** were a [sentient species](#) characterized by their small size and head shaped like a pair of [macrobinoculars](#). Known Xot included [Bidvel](#) and [Davail](#), who operated a [scrap pile](#).

Contents [\[hide\]](#)

- 1 [Biology and appearance](#)
- 2 [Xot in the galaxy](#)
- 3 [Appearances](#)
- 4 [Notes and references](#)

Biology and appearance [edit](#) | [edit source](#)

The Xot^[4] were small-sized, with heads shaped like a pair of [macrobinoculars](#). They had large feet, four-fingered hands that included an opposable thumb, two feelers above the [nostrils](#), and two other feelers dangling from under their large [eyes](#). Their skin varied in hue, from [gray-blue](#)^[1] to pink.^[2] or even red.^[3] Similarly, their irises came in a variety of colors, including green, pink,^[1] and red.^[3]

Xot in the galaxy [edit](#) | [edit source](#)

In the third [year](#) before the [Battle of Yavin](#),^[5] the Xot [Bidvel](#) and [Davail](#) were running a [scrap pile](#) on a [remote planetoid](#).^[1] In the second year before the Battle of Yavin,^[6] on the [day](#) that [Hera Syndulla](#), [Garazeb Orrelios](#), and [Rex](#) rescued [Ketsu Onyo](#) from the [Starlag XIX](#) space-bound [prison](#), there was at least one Xot [inmate](#) there.^[3]

Appearances [edit](#) | [edit source](#)

- **REBELS** "Escaping the Scrap Pile"—*Star Wars Rebels Magazine* 19 (First appearance)
- **REBELS** "Final Round"—*Star Wars Rebels Magazine* 34
- **REBELS** "Fifth and Final"—*Star Wars Rebels Magazine*



Biological classification
Designation
Physical characteristics
Skin color
Eye color

draft-ietf-dprive-xfr-over-tls-07 - Chromium

draft-ietf-dprive-xfr-over- x +

datatracker.ietf.org/doc/html/draft-ietf-...

[\[Search\]](#) [\[txt\]](#) [\[pdf\]](#) [\[bibtex\]](#) [\[Tracker\]](#) [\[WG\]](#) [\[Email\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Nits\]](#)

Versions: [\(draft-hzpa-dprive-xfr-over-tls\) 00 01](#) Standards Track
[02](#) [03](#) [04](#) [05](#) [06](#) [07](#)

dprive W. Toorop
Internet-Draft NLnet Labs
Updates: [1995](#), [5936](#), [7766](#) (if approved) S. Dickinson
Intended status: Standards Track Sinodun IT
Expires: August 20, 2021 S. Sahib
P. Aras
A. Mankin
Salesforce
February 16, 2021

DNS Zone Transfer-over-TLS
draft-ietf-dprive-xfr-over-tls-07

Abstract

DNS zone transfers are transmitted in clear text, which gives attackers the opportunity to collect the content of a zone by eavesdropping on network connections. The DNS Transaction Signature (TSIG) mechanism is specified to restrict direct zone transfer to authorized clients only, but it does not add confidentiality. This document specifies the use of TLS, rather than clear text, to prevent zone content collection via passive monitoring of zone transfers: XFR-over-TLS (XoT). Additionally, this specification updates [RFC1995](#), [RFC5936](#) and [RFC7766](#).

Status of This Memo

Pink, green,^[1] red^[3]

[Source]

^H^H^HXoT

The **Xot** were a **sentient species** characterized by their small size and head shaped like

Contents

- 1 Biology and ap
- 2 Xot in the gala
- 3 Appearances
- 4 Notes and refe

The Xot^[4] were s
macrobinoculars
included an oppo
other feelers dan
hue, from gray-b
came in a variety

In the third year I
were running a s
before the Battle
Orrelios, and Re
bound prison, the

- **REBELS** "E" 19 (First appearance)
- **REBELS** "F" 19 (First appearance)
- **REBELS** "F" 19 (First appearance)

Status:	Proposed Standard			
More info:	Datatracker IPR Info page			
Stream:	Internet Engineering Task Force (IETF)			
RFC:	8914			
Category:	Standards Track			
Published:	October 2020			
ISSN:	2070-1721			
Authors:	W. Kumari <i>Google</i> D. Lawrence <i>Salesforce</i>	E. Hunt <i>ISC</i>	R. Arends <i>ICANN</i>	W. Hardaker <i>USC/ISI</i>

Abstract

This document defines an extensible method to return additional information about the cause of DNS errors. Though created primarily to extend SERVFAIL to provide additional information about the cause of DNS and DNSSEC failures, the Extended DNS Errors option defined in this document allows all response types to contain extended error information. Extended DNS Error information does not change the processing of RCODEs.

draft-ietf-dprive-xfr-over-tls-07 - Chromium

draft-ietf-dprive-xfr-over-tls-07

datatracker.ietf.org/doc/html/draft-ietf-...

[\[tex\]](#) [\[Tracker\]](#) [\[WG\]](#) [\[Email\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Nits\]](#)

[draft-ietf-dprive-xfr-over-tls-07](#) Standards Track

W. Toorop
NLnet Labs
S. Dickinson
Sinodun IT
S. Sahib
P. Aras
A. Mankin
Salesforce
February 16, 2021

DNS Zone Transfer-over-TLS

draft-ietf-dprive-xfr-over-tls-07

are transmitted in clear text, which gives opportunity to collect the content of a zone by network connections. The DNS Transaction Signature is specified to restrict direct zone transfer to only, but it does not add confidentiality. This is the use of TLS, rather than clear text, to prevent eavesdropping on passive monitoring of zone transfers. Additionally, this specification updates RFC7766.

IETF 110 Hackathon planning - XoT Implementation - Google Docs - Chromium

IETF 110 Hackathon planning - XoT Implementation

This document is intended as a braindump of potential activities for XoT that could happen at the IETF 110 Hackathon.

Area	What	Who
Implementation		
NSD	Finish and test connection reuse PR (https://github.com/NLnetLabs/nsd/pull/145) - Handle NSD primary connection shut - Implement Keepalive (client side and also need server side for testing) - Add unit tests	Sara/Shivan/NLnetLabs
NSD	Finish and test XoT PR (https://github.com/NLnetLabs/nsd/pull/149) - Handle handshake hang when far ends listens on TCP but not TLS - Fix <code>confcheck</code> unit test - Add unit tests	Sara/Shivan/NLnetLabs
NSD	Server side work <code>Config option</code> to serve zone over XoT only (and to also require IP based ACL) - Implement EDE? (Tom Carpay?) - Keep-alive edns0	Han/Pallavi
BIND	Talk to Ondrej about interop testing the 9.17.10 XoT implementation?	
PowerDNS	Talk to Peter about implementation	
Knot	Talk to Libor about implementation	
Testing		
Interop	We have NSD and BIND client side and server side NSD and BIND support DoT and we can use a proxy in front of PowerDNS or Knot that could be interop tested.... (2 clients x 4 servers matrix at the moment?) - Should we consider setting up test zones (delegated from dnsprivacy.com?) for public testing? (How/iff to apply IP based ACLs?). Willem may be able to help by providing servers similar to those used for the catalogue zones testing in the previous hackathon.... - Or create a standalone test harness to do this?	
Load testing	Show increase in server load when using XoT instead of XFR-over-TCP for a heavily loaded server?	
Libraries		

Comments:

Pallavi Aras 4:45 PM Feb 25
[@willem@nlnetlabs.nl](mailto:willem@nlnetlabs.nl)
[@sara@sinodun.com](mailto:sara@sinodun.com), Should this be a config option at zone-level or at primary server -level?

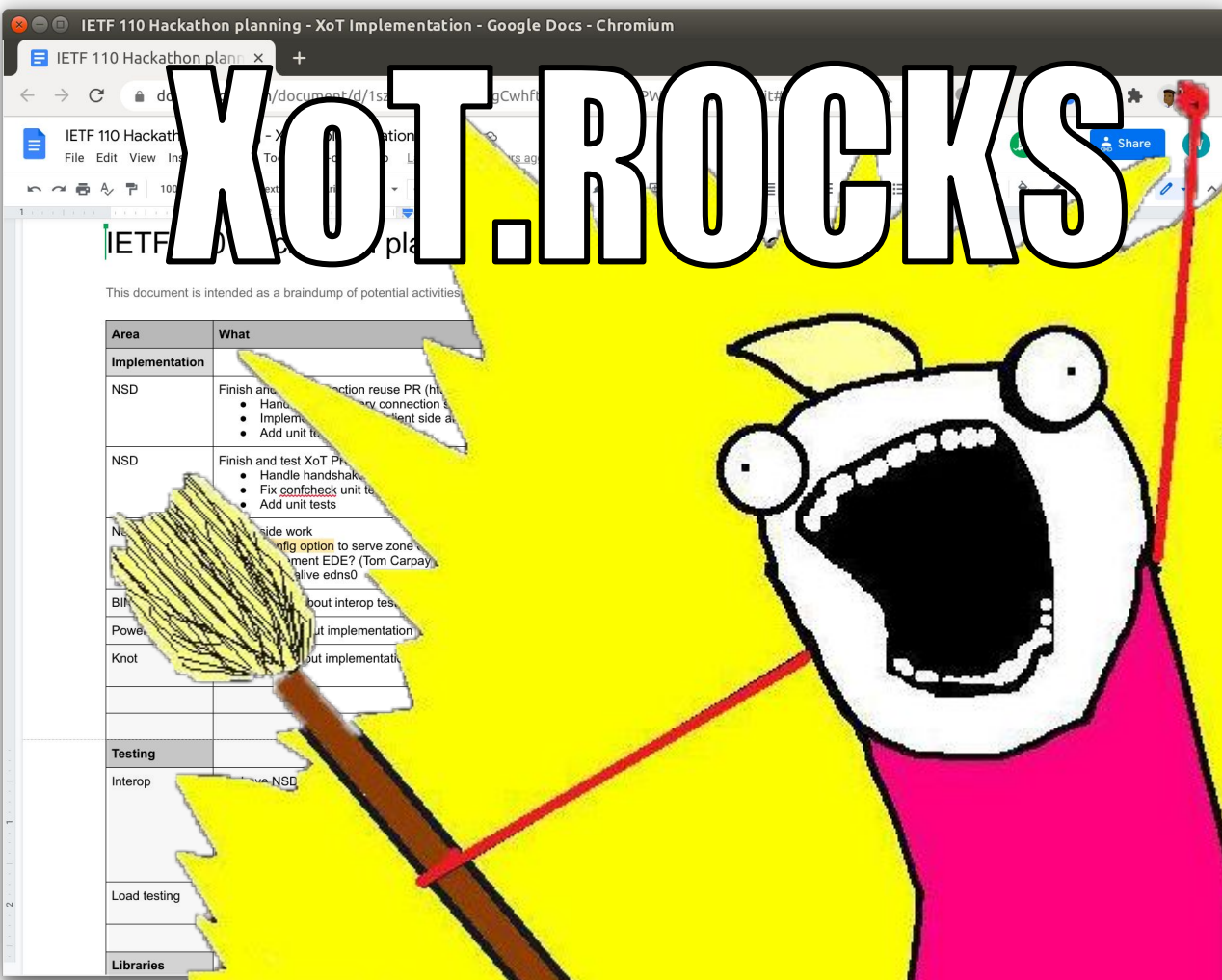
Willem Toorop 5:45 PM Feb 25
 Good question!
 Maybe an extra option argument on the "provide-xfr" option?
[Show all 5 replies](#)

Willem Toorop 4:33 PM Yesterday
[@Pallavi](#) have you started with this?

Pallavi Aras 4:56 PM Yesterday
 I have started some work but based on our discussion I will add some modifications

H^H^H XoT

- Sara Dickinson
- Shivan Kaul Shahib
- Pallavi Aras
- Han Zhang
- Tom Carpay (EDE)
- Wouter Wijngaards (all on NSD)
- Peter van Dijk (PowerDNS)
- Matthijs Mekking (ISC BIND)



XoT.ROCKS

HALL OF XoT

Ara Dickinson
Shivan Kaul Shahib

- Pallavi Aras
- Han Zhang
- Tom Carpay (EDE)
- Wouter Dijkstra (NSD)

er van Dijk
(NSD)

Mekking
(NSD)

Ha

XoT

inson

ul Shahib

as

g

ay (EDE)

ngaards

(SD)

Dijk

(S)

Mekking

(SD)

IETF 110 Hackathon planning - XoT Implementation - Google Docs - Chromium

IETF 110 Hackathon plann x +

docs.google.com/document/d/1szbKPB4ij-8LnVbg...
IETF 110 Hackathon planning - XoT Implementation
File Edit View Insert Format Tools Add-ons Help See new changes

100% Normal text Arial 11 B I U A

VMS for use in hackathon:

name	Internal IPv4	Public IPv4	IPv6	Role/Purpose
ns1.xot.rocks	172.31.34.138	3.126.83.50	2a05:d014:d33:2020::1111	Primary NSD server for XoT.rocks domain, available for transfer over XoT only.
ns2.xot.rocks	172.31.39.106	54.93.249.195	2a05:d014:d33:2020::2222	Secondary NSD server for XoT.rocks domain.
ns3.xot.rocks	172.31.33.27	35.156.42.41	2a05:d014:d33:2020::3333	Bind (secondary?) by Mattheijs Mekking
ns4.xot.rocks	172.31.43.222	52.59.193.53	2a05:d014:d33:2020::4444	PowerDNS XoT secondary voor XoT.rocks domain by @habbie
ns5.xot.rocks	172.31.36.89	54.93.85.250	2a05:d014:d33:2020::5555	Bind (primary?) by Mattheijs Mekking

What got done

- Extended DNS Errors (Tom Carpay)
 - Found some potential new EDE codes
 - For example name overflow with DNAME expansion

●

●

●

What got done

- ACL to provide zones XoT only (Pallavi Aras and Han Zhang)

- AC

```
remote-control:
  control-enable: yes
```

```
zone:
```

```
  name:          "xot.rocks"
  zonefile:      "%s.signed"
  provide-xfr:   TLS      0.0.0.0/0      NOKEY
  provide-xfr:   TLS      ::0/0         NOKEY
```

```
~
```

```
29,2-9
```

```
Bodem
```

```
willem@makaak: ~/repos/nsd 80x13
willem@makaak:~/repos/nsd$ ./nsd-checkconf nsd.conf
nsd.conf:28: error: Either a TSIG key or a specific address or address range MUST be specified if TLS option is set
nsd.conf:29: error: Either a TSIG key or a specific address or address range MUST be specified if TLS option is set
read nsd.conf failed: 2 errors in configuration file
willem@makaak:~/repos/nsd$
```

s
hang)

- AC

```
willem@makaak: ~/repos/nsd
remote-control:
    control-enable: yes

zone:
    name:                "xot.rocks"
    zonefile:            "%s.signed"
    provide-xfr:         TLS      0.0.0.0/1      NOKEY
    provide-xfr:         TLS      128.0.0.0/1     NOKEY
    provide-xfr:         TLS      ::0/1          NOKEY
    provide-xfr:         TLS      8000::0/1       NOKEY
"nsd.conf" 31L, 614C opgeslagen                               31,1-8      Bodem

willem@makaak: ~/repos/nsd 80x11
willem@makaak:~/repos/nsd$ ./nsd-checkconf nsd.conf
willem@makaak:~/repos/nsd$ kdig @ns1.xot.rocks xot.rocks AXFR +tls
;; AXFR for xot.rocks.
xot.rocks.      3600      IN      SOA      ns1.xot.rocks. sysadm.nlnetlabs.
nl. 1615410822 14400 1800 2419200 300
xot.rocks.      3600      IN      RRSIG     SOA 15 2 3600 20220310211342 202
10310211342 24485 xot.rocks. huVa5rIvQFZKDCx+VibTAH8WZfW9184r9f802UWjouHSRxnypEN
xcLdPWJii1oczz1CMEBQumGwDOPjfqgSPCw==
xot.rocks.      3600      IN      RRSIG     A 15 2 3600 20220310211342 20210
310211342 24485 xot.rocks. yX9J0cI5bJCXlWyNBUqZ/smYzGMySvhex/s0xSWYIyZckggUg03ee
VBCMDmcUvShZn8BQJgn4n3U+Ca09V0PDA==
xot.rocks.      3600      IN      RRSIG     NS 15 2 3600 20220310211342 2021
0310211342 24485 xot.rocks. Byodt+SDq+j5JUUrRrZ00Ba6d50G8Pz1rqFtg70QWrjoZVbLbbqQ
```

s
hang)

What got done

- ACL to provide zones XoT only (Pallavi Aras and Han Zhang)
- ACL for queries (Willem Toorop)

- AC

- AC

```
willem@makaak: ~/repos/nsd
zone:
name: "xot.rocks"
zonefile: "%s.signed"
provide-xfr: TLS 0.0.0.0/1 NOKEY
provide-xfr: TLS 128.0.0.0/1 NOKEY
provide-xfr: TLS ::0/1 NOKEY
provide-xfr: TLS 8000::0/1 NOKEY
allow-query: 0.0.0.0/0 BLOCKED
allow-query: ::0/0 BLOCKED
34,29-55 Bodem

willem@makaak: ~/repos/nsd 80x13
willem@makaak:~/repos/nsd$ kdig @ns1.xot.rocks xot.rocks SOA +tls
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(RSA-PSS-RSAE-SHA256)-(AES-256-GCM)
;; ->HEADER<- opcode: QUERY; status: REFUSED; id: 54451
;; Flags: qr rd; QUERY: 1; ANSWER: 0; AUTHORITY: 0; ADDITIONAL: 1
;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1232 B; ext-rcode: NOERROR
;; Option (15): 0015
;; QUESTION SECTION:
;; xot.rocks. IN SOA
;; Received 44 B
```

s
hang)

prop)

What got done

- ACL to provide zones XoT only (Pallavi Aras and Han Zhang)
- ACL for queries (Willem Toorop)
- rcode: REFUSED, EDE: 20 (Not Authoritative)
For all errors with XoT zones that may not be queried?

SOA query over DoT too

Serials can be signaled by catalog zones (NO NOTIFY)

What got done

- XoT transfers between NSD, PowerDNS & BIND
(Peter van Dijk , Matthijs Mekking, Willem Toorop)



OR

NSD

NSD

Krill

IETF 110 Hackathon planning - XoT Implementation - Google Docs - Chromium

IETF 110 Hackathon planning x +

docs.google.com/document/d/1szbKPB4ij-8LnVbg... ☆

IETF 110 Hackathon planning - XoT Implementation ☆

File Edit View Insert Format Tools Add-ons Help See new changes

100% Normal text Arial 11 B I U A

VMS for use in hackathon:

name	Internal IPv4	Public IPv4	IPv6	Role/Purpose
ns1.xot.rocks	172.31.34.138	3.126.83.50	2a05:d014:d33:2020::1111	Primary NSD server for XoT.rocks domain, available for transfer over XoT only.
ns2.xot.rocks	172.31.39.106	54.93.249.195	2a05:d014:d33:2020::2222	Secondary NSD server for XoT.rocks domain.
ns3.xot.rocks	172.31.33.27	35.156.42.41	2a05:d014:d33:2020::3333	Bind (secondary?) by Matthijs Mekking
ns4.xot.rocks	172.31.43.222	52.59.193.53	2a05:d014:d33:2020::4444	PowerDNS XoT secondary voor XoT.rocks domain by @habbie
ns5.xot.rocks	172.31.36.89	54.93.85.250	2a05:d014:d33:2020::5555	Bind (primary?) by Matthijs Mekking

What we learned

- From EDE - Maybe an update on RFC8914 with new Codes?
- Privacy works best with XoT and Catalog Zones and EDE combined
- XoT just works^H^H^H^H^HRocks

Wrap Up

Team members:

- Sara Dickinson
- Shivan Kaul Sahib
- Pallavi Aras
- Han Zhang
- Tom Carpay
- Wouter Wijngaards
- Peter van Dijk
- Matthijs Mekking
- Willem Toorop

First timers @ IETF/Hackathon:

- Tom Carpay