TLS ♥ DNS ♥ Tor

equinox

31C3, Hamburg, 2014-12-30

wtf is this shit?

- this is not a crypto talk
- this is not a DNSsec talk

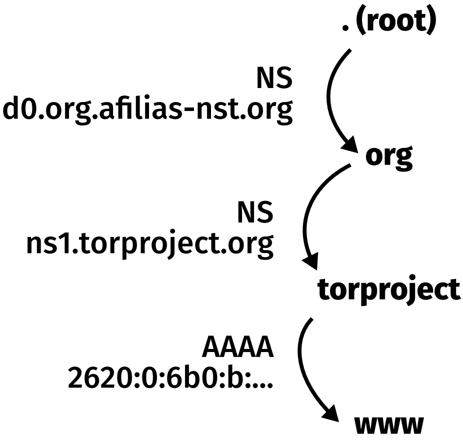
wtf is this shit?

- this is not a crypto talk
- this is not a DNSsec talk
- this is a layer 9 talk

okay?

- please do DNSsec and DANE
- they’re good things and here’s why

DNSsec and DANE in 60 seconds



. (root)

NS
d0.org.afilias-nst.org

org

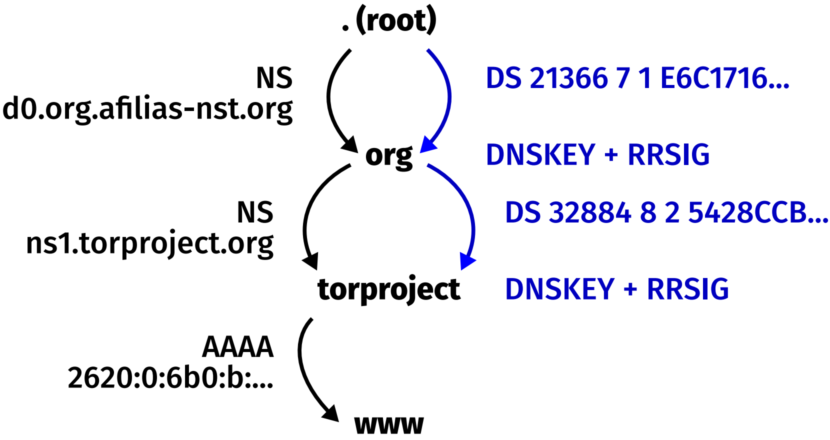
NS
ns1.torproject.org

torproject

AAAA
2620:0:6b0:b:...

www

DNSsec and DANE in 60 seconds



. (root)

NS
d0.org.afilias-nst.org

DS 21366 7 1 E6C1716...

org

DNSKEY + RRSIG

NS
ns1.torproject.org

DS 32884 8 2 5428CCB...

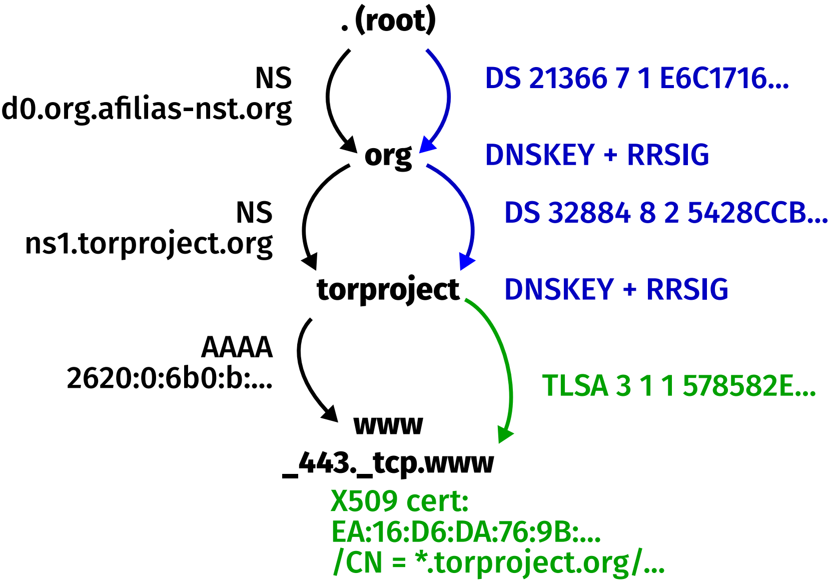
torproject

DNSKEY + RRSIG

AAAA
2620:0:6b0:b:...

www

DNSsec and DANE in 60 seconds



. (root)

NS
d0.org.afilias-nst.org

DS 21366 7 1 E6C1716...

org

DNSKEY + RRSIG

NS
ns1.torproject.org

DS 32884 8 2 5428CCB...

torproject

DNSKEY + RRSIG

AAAA
2620:0:6b0:b:...

TLSA 3 1 1 578582E...

www

_443._tcp.www

X509 cert:
EA:16:D6:DA:76:9B:...
/CN = *.torproject.org/...

Issues

- DNSsec as a protocol sucks
- ICANN has the root keys
- TLD operator has TLD keys
- NSA/... can request keys

Issues

- DNSsec as a protocol sucks
- ICANN has the root keys
- TLD operator has TLD keys
- NSA/... can request keys
  and attack your internet connection

Trust relations

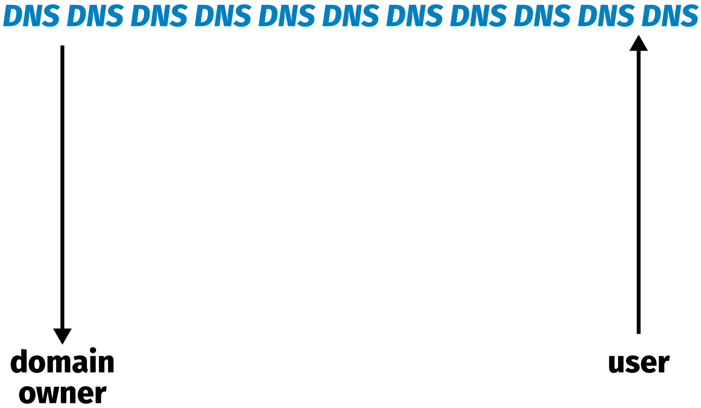
After forcing the TLD operator to hand over their keys, the NSA can go break your internet wire and MitM on the DNSsec replies

Or they just tell the TLD operator to give different replies to you (or everyone).

But.

- single hierarchy
- online system

DNSsec ♥ Tor

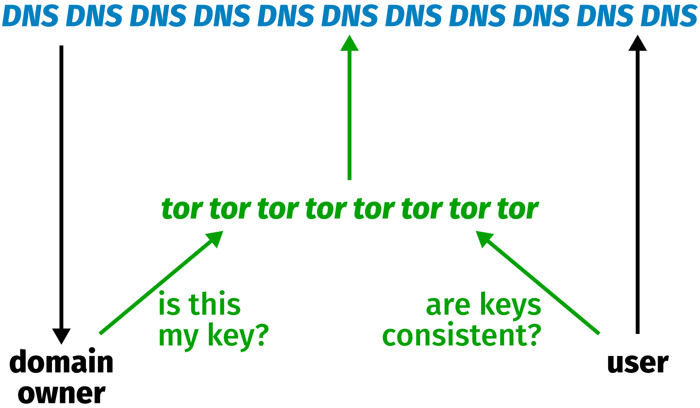


DNS DNS DNS DNS DNS DNS DNS DNS DNS DNS DNS

domain owner

user

DNSsec ♥ Tor



DNS DNS DNS DNS DNS DNS DNS DNS DNS DNS DNS

tor tor tor tor tor tor tor tor

is this my key?

are keys consistent?

domain owner

user

Whoop Whoop Whoop

- using Tor as common base
- hopefully, targeting individual Tor users across multiple requests is difficult
- Owner checks info in Tor,
  User checks info in Tor

Whoop Whoop Whoop

- using Tor as common base
- hopefully, targeting individual Tor users across multiple requests is difficult
- Owner checks info in Tor,
  User checks info in Tor
- additional trust chain

DNSsec and DANE pretty-please!

- Firefox & Chrome: boo!
- postfix & irssi: yay!

- needs domain owners’ action
- needs registrars’ action
- could use special DNS support in Tor

Play with the tools we have

No new protocol in this talk, no new crypto algorithm, no X509 extensions.

Just creativity with existing tools!

kthxbai

Fuck the X509 CA scheme.

questions?
equinox@diac24.net