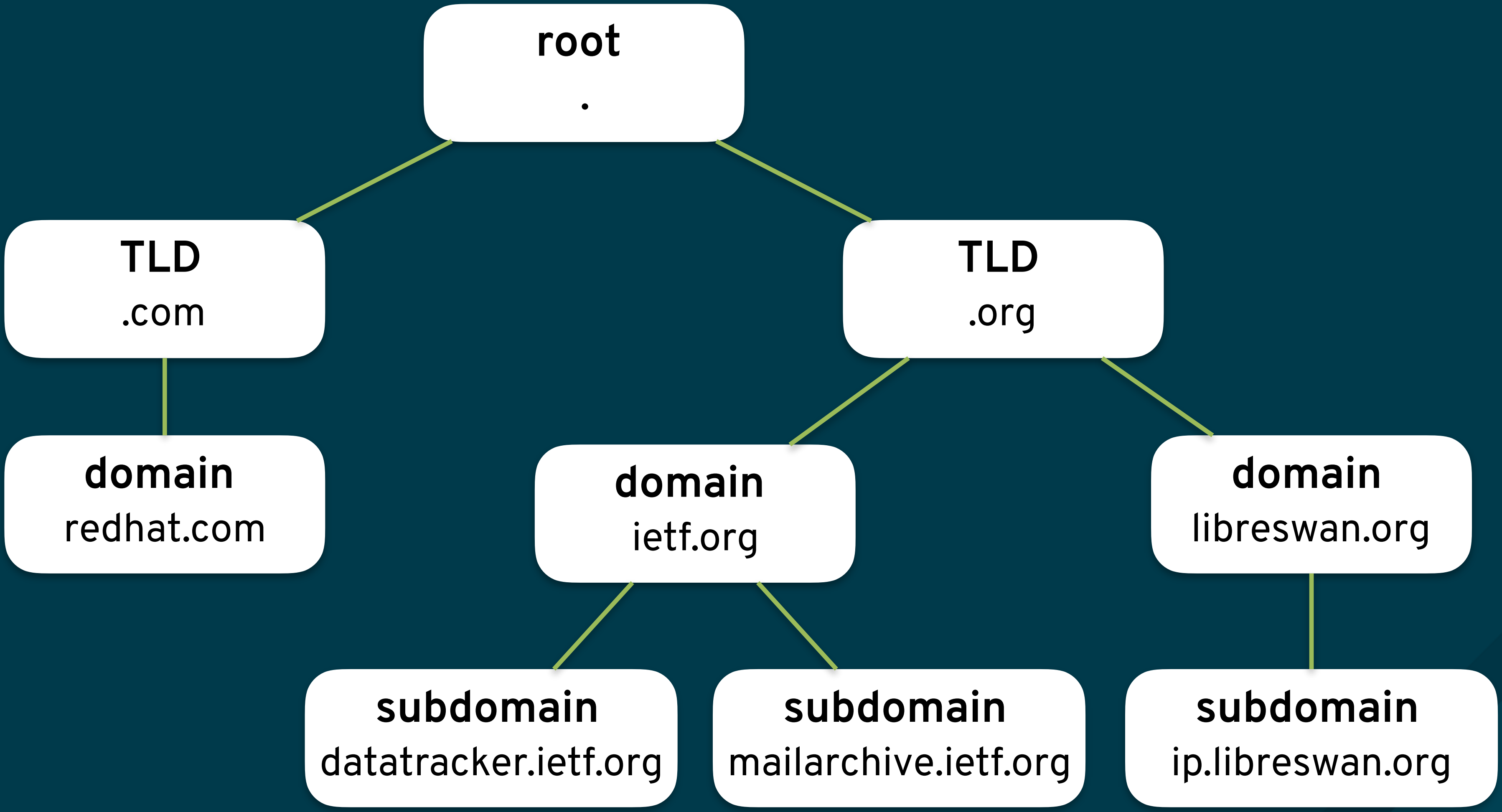
redhat

Increasing the Trust of the DNS Hierarchy

ICANN DNS Symposium
Montreal - July 13, 2018

Paul Wouters
RHEL Security

Hierarchical trust using DNS



root

.

TLD

.com

TLD

.org

domain

redhat.com

domain

ietf.org

domain

libreswan.org

subdomain

datatracker.ietf.org

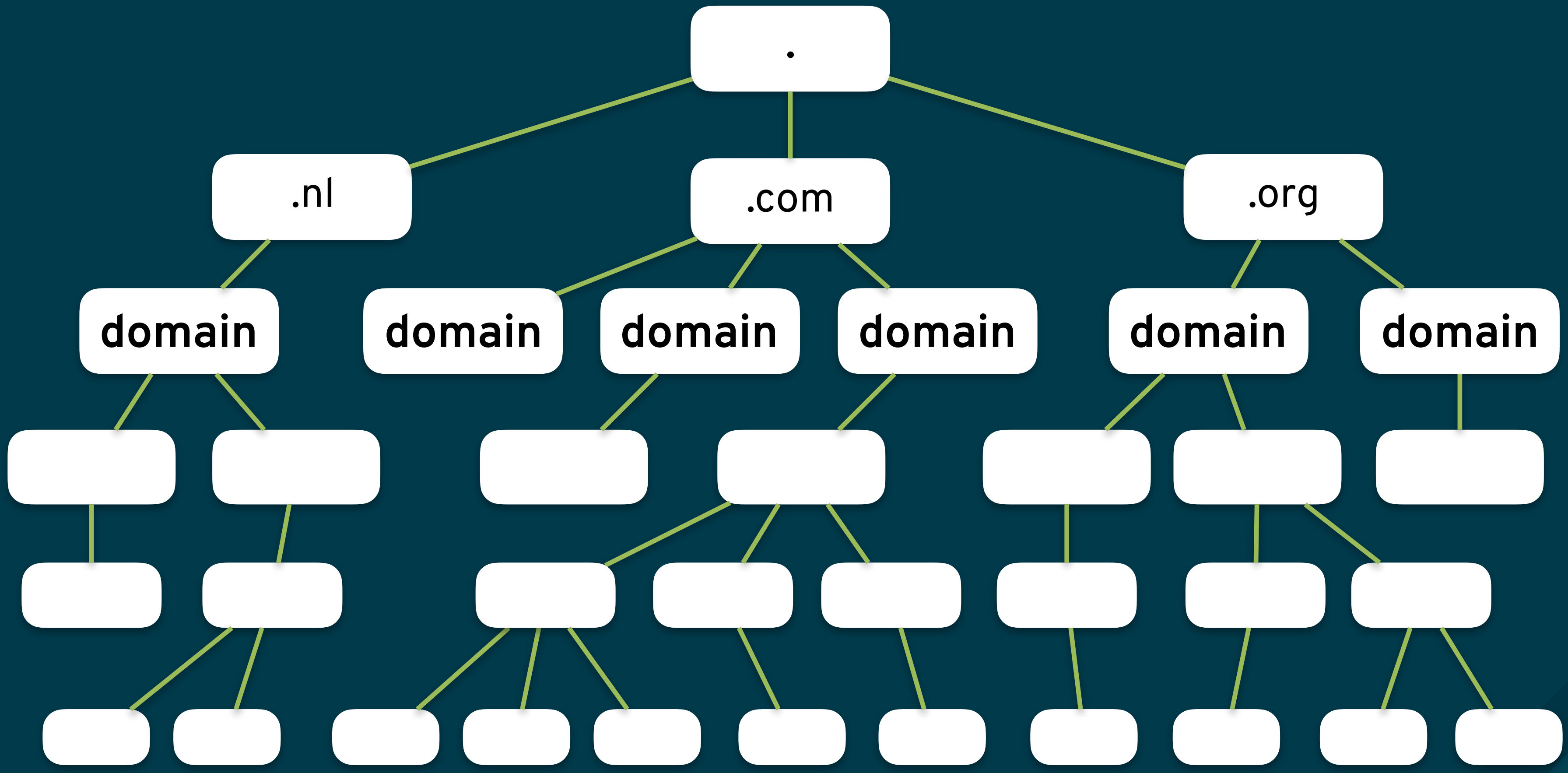
subdomain

mailarchive.ietf.org

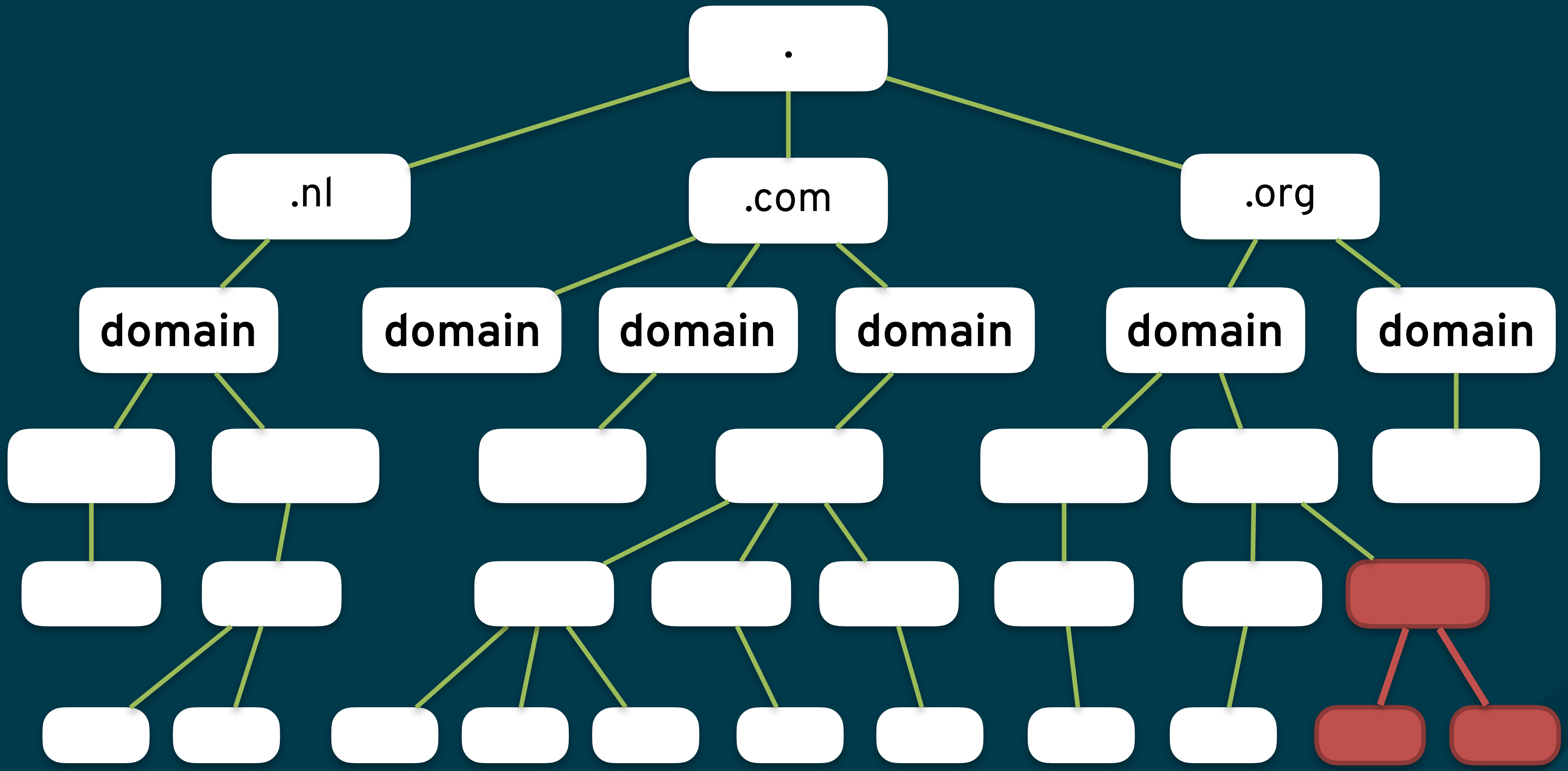
subdomain

ip.libreswan.org

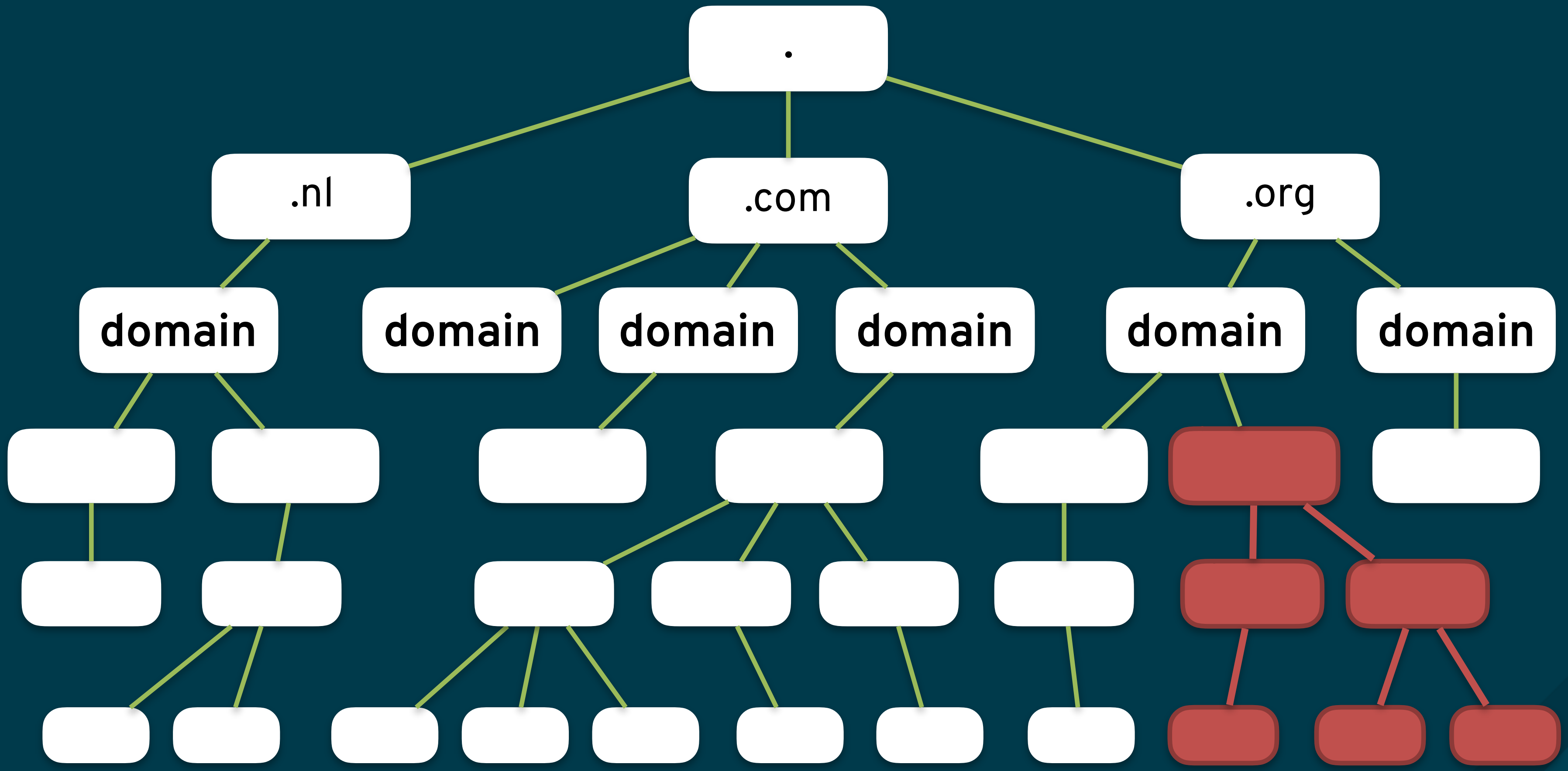
Hierarchical trust using DNS



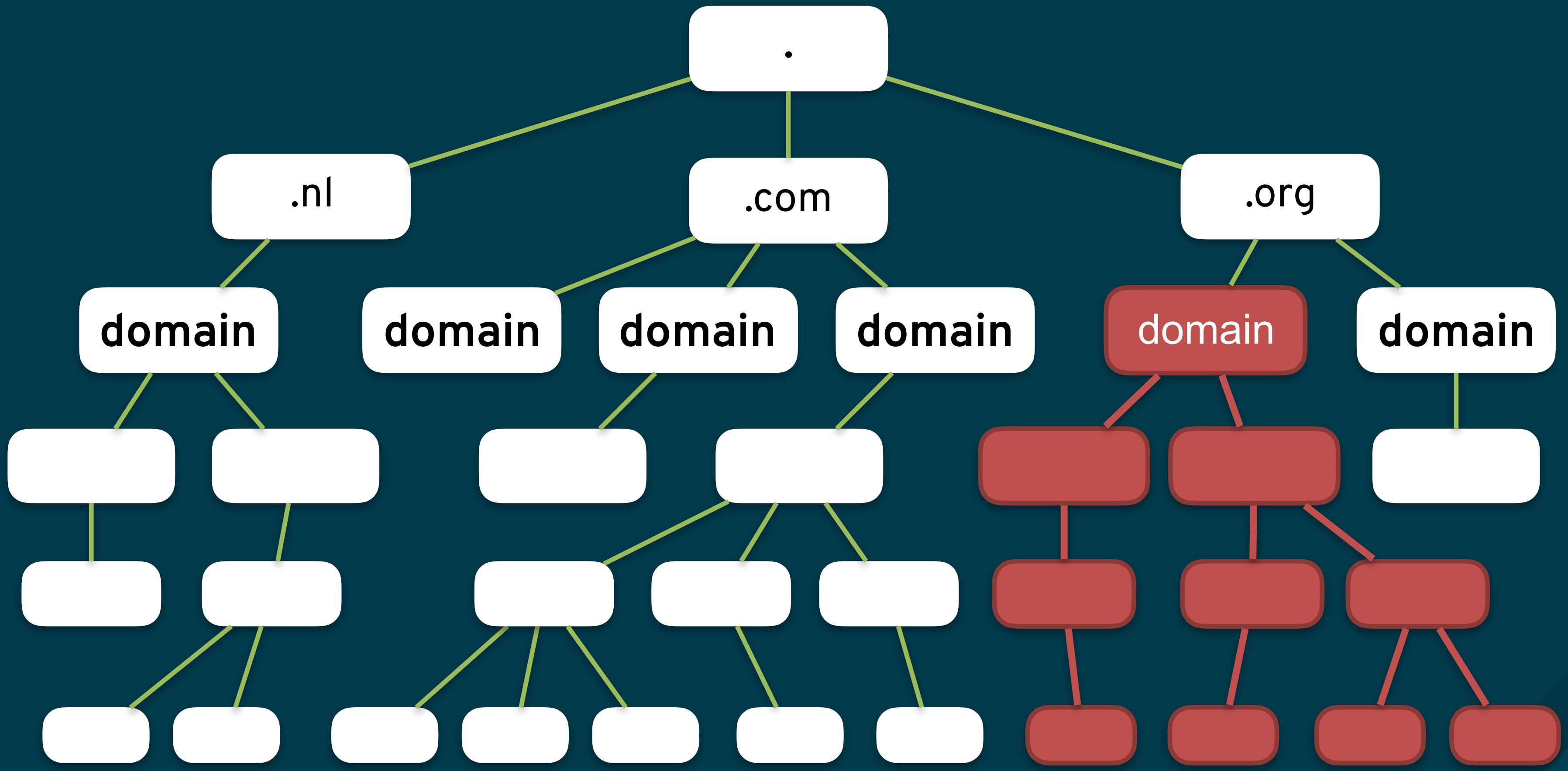
A parent has full authority over its children



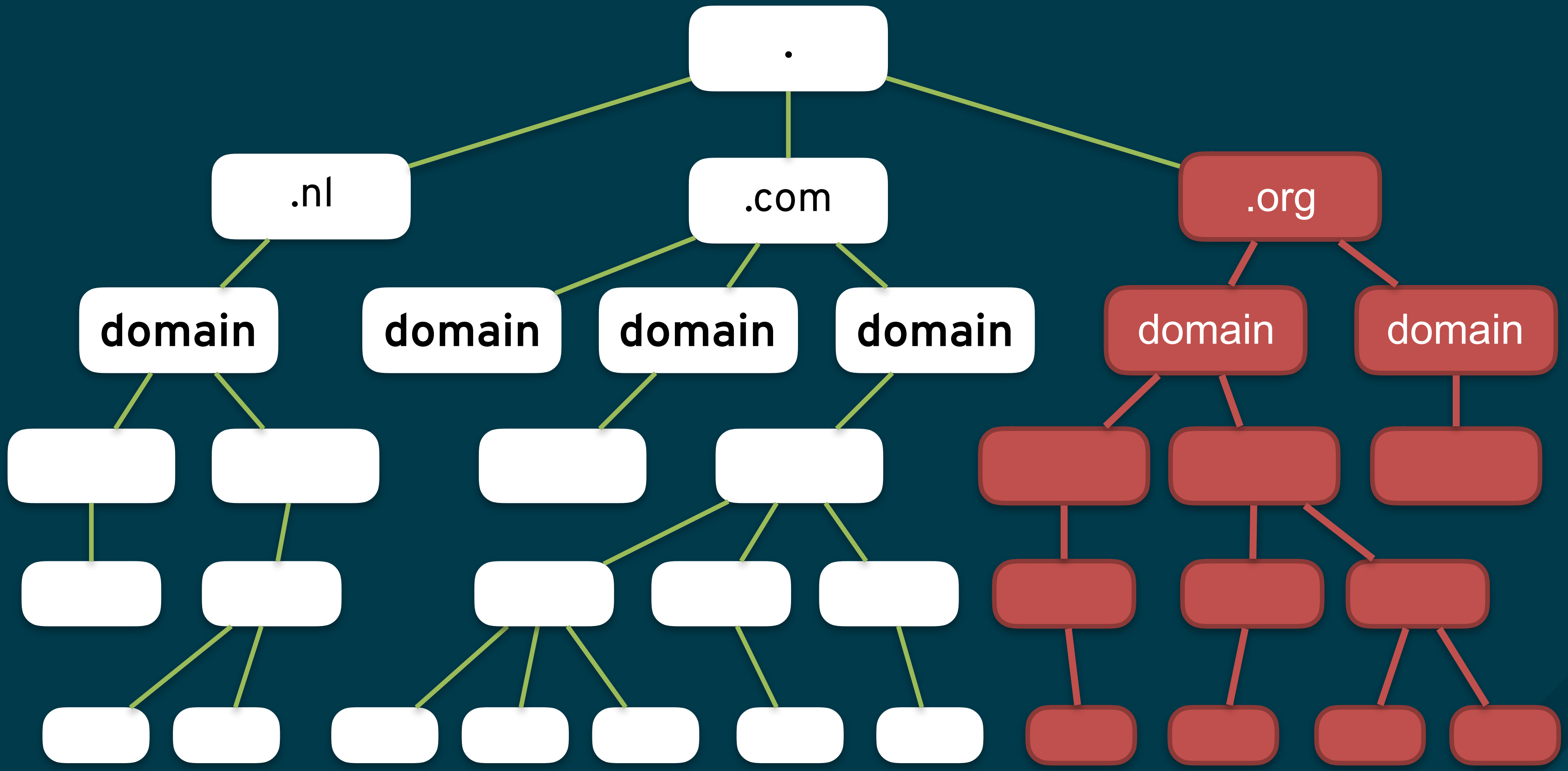
The grand children are at the mercy of their grand parent



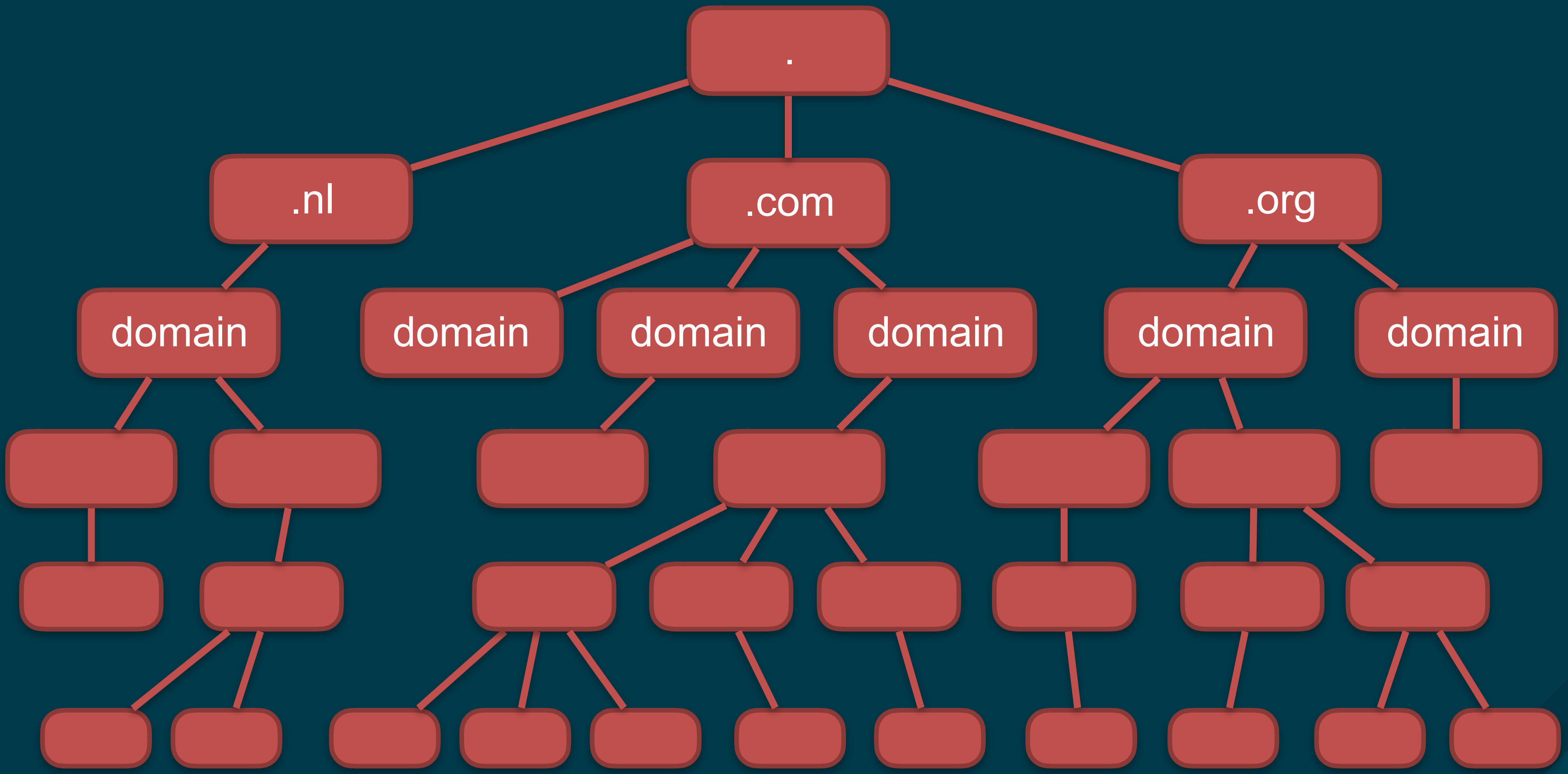
With great power comes .....



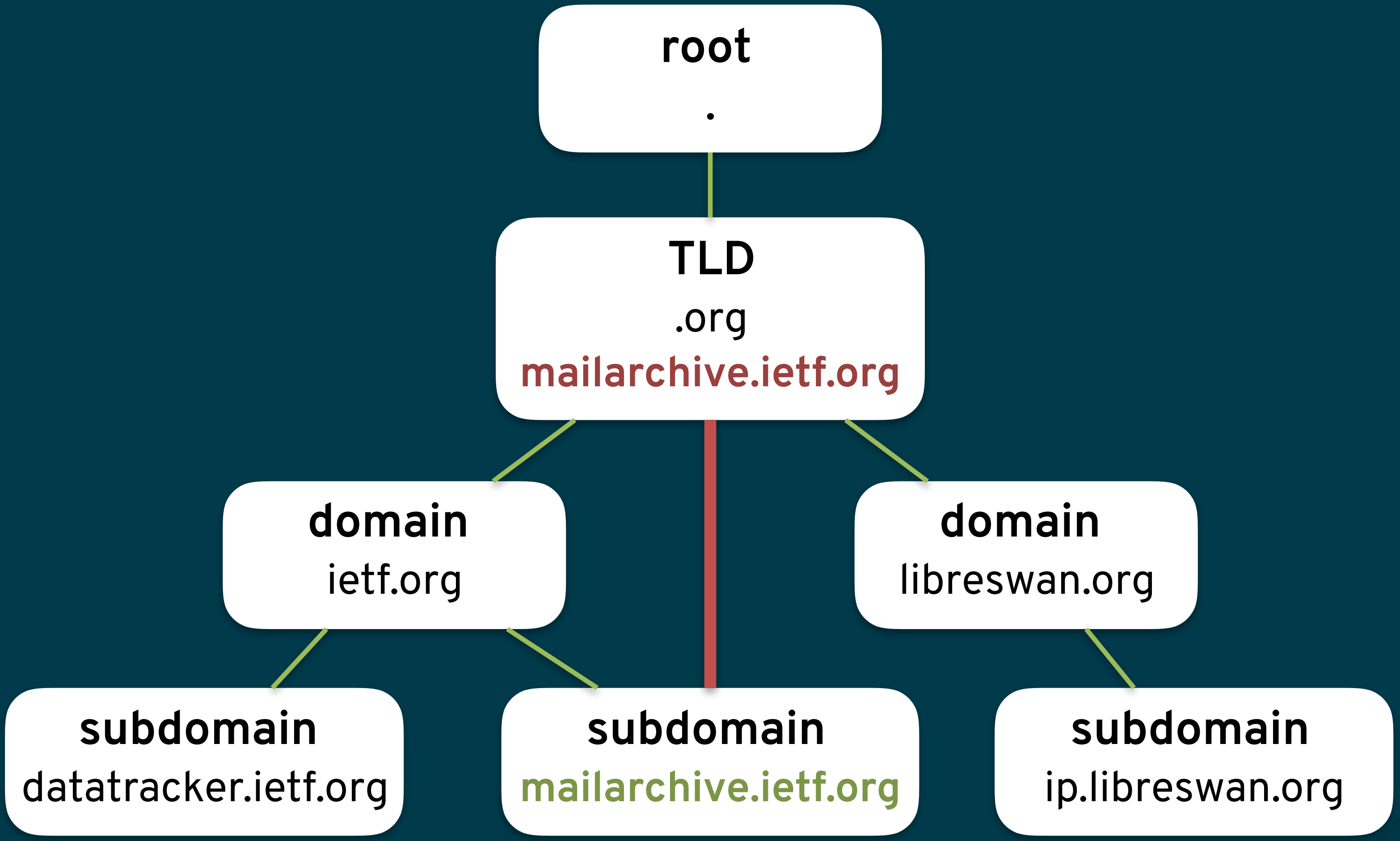
.... Great responsibility



The root of all (dis)trust



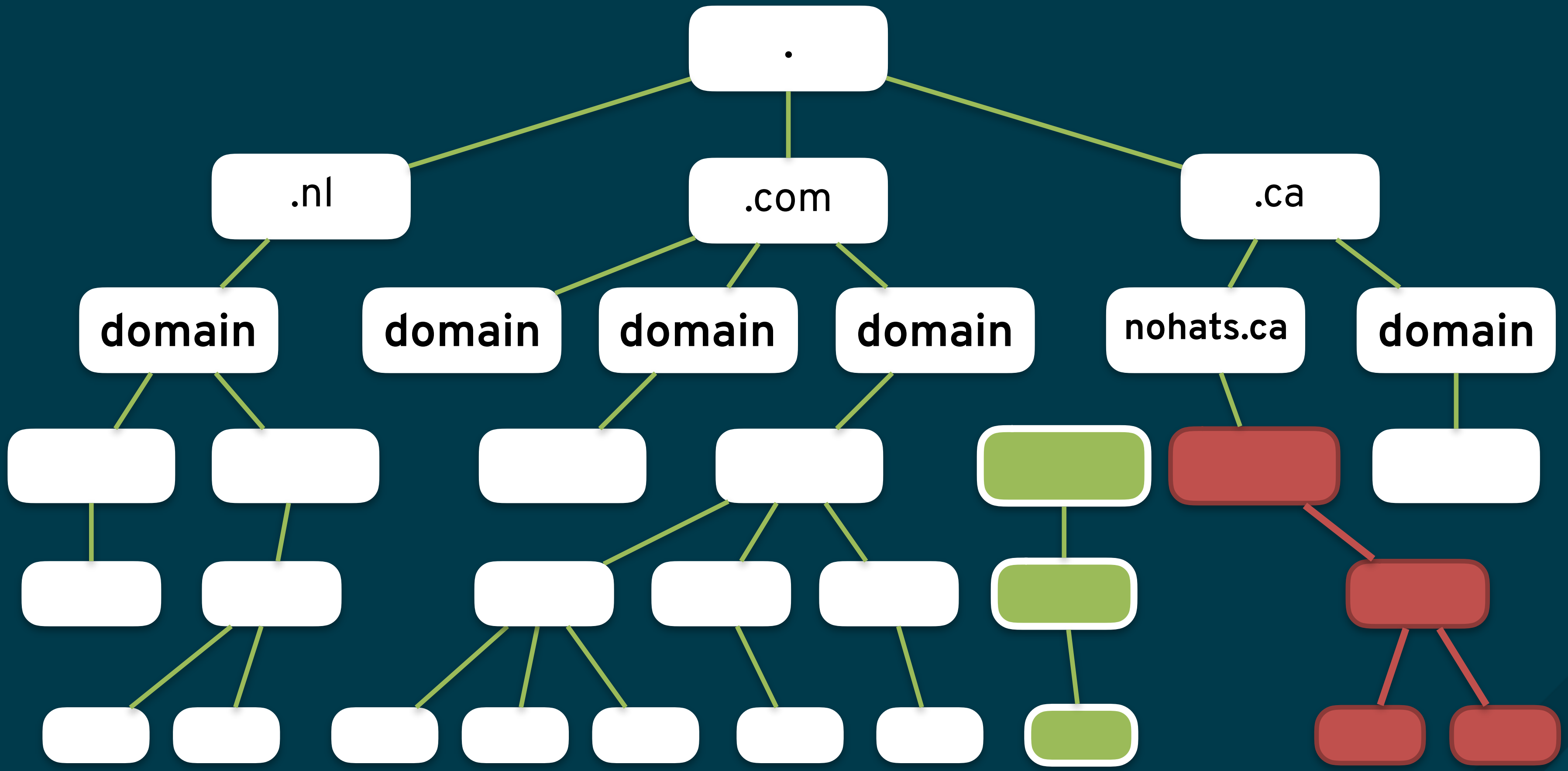
Attack 1: Parental override of delegation



Attack 1: Parental override of delegation

```
                ......
   ottawa.nohats.ca. IN NS travelagent.com.
powerbind.nohats.ca. IN NS ns1.trusted.com.
powerbind.nohats.ca. IN DS 17869 8 2 f22bb[...]
powerbind.nohats.ca. IN RRSIG DS 8 3 3600 […]
  toronto.nohats.ca. IN NS ns1.bighoster.ca.
                ......
_443._tcp.powerbind.nohats.ca. IN TLSA 3 1 1 302BBD0
_443._tcp.powerbind.nohats.ca. IN RRSIG TSLA 8 3 3600 […]
```

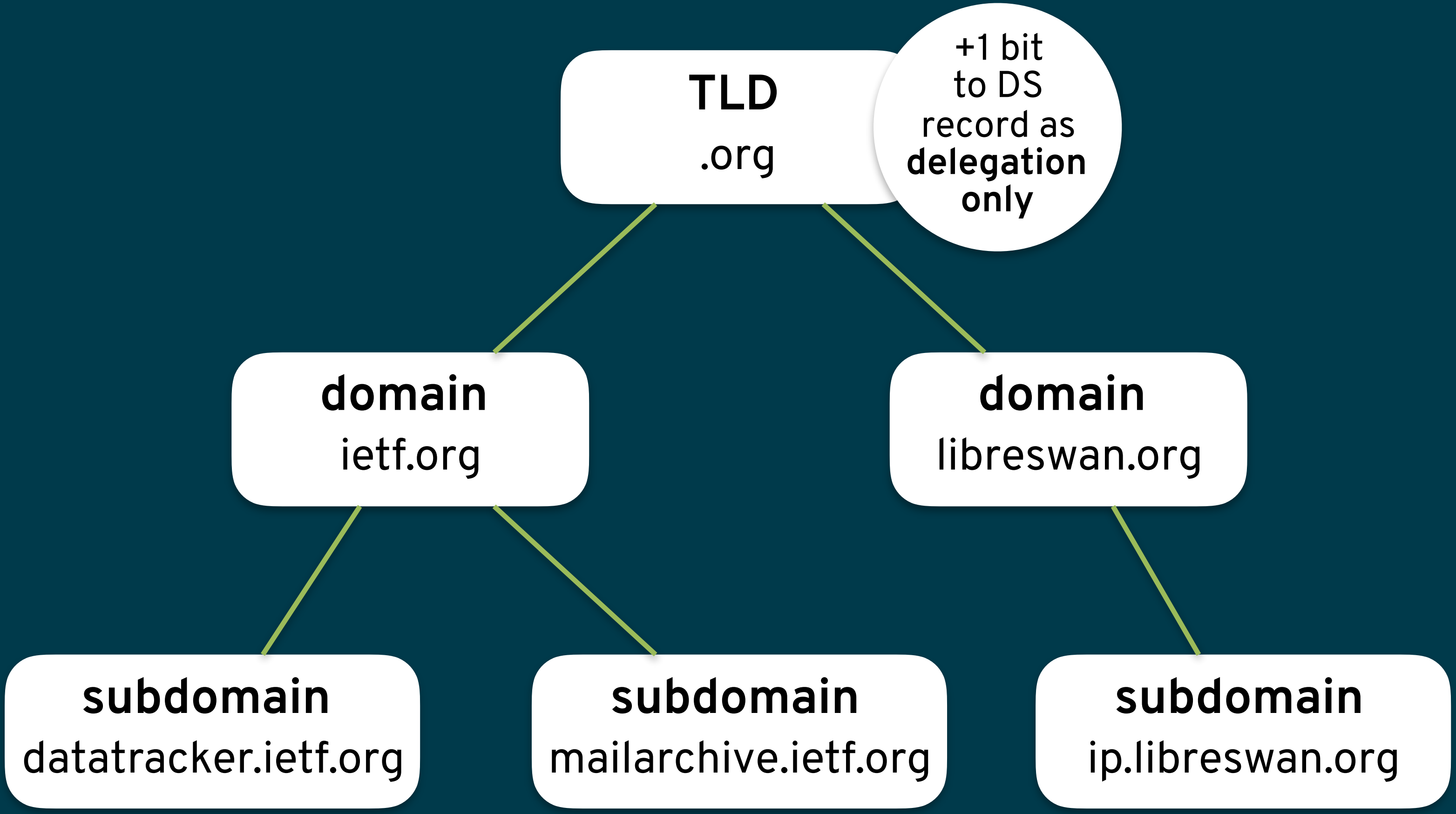
Attack 2) Replacing child delegation



Attack 2) Replacing child delegation

```
                ......
   ottawa.nohats.ca. IN NS travelagent.com.
; powerbind.nohats.ca. IN NS ns1.trusted.com.
powerbind.nohats.ca. IN NS ns0.evil.com.
; powerbind.nohats.ca. IN DS 17869 8 2 f22bb[…]
powerbind.nohats.ca. IN DS 98765 8 2 aaabbbccc[...]
powerbind.nohats.ca. IN RRSIG DS 8 3 3600 […]
  toronto.nohats.ca. IN NS ns1.bighoster.ca.
                ......
```

The solution:
The DNSKEY DELEGATION_ONLY flag



TLD
.org

+1 bit to DS record as **delegation only**

domain
ietf.org

domain
libreswan.org

subdomain
datatracker.ietf.org

subdomain
mailarchive.ietf.org

subdomain
ip.libreswan.org

DELEGATION_ONLY flag benefits:

1) Public commitment by parent to be a delegation-only zone to prevent rogue parents from deep-signing child data.

   - Publish commitment via DNSKEY flag

2) DNSSEC transparency that does not require logging ALL DNS records with public keys

   - With above flag, we only need to log DNSKEY / DS records or their NSECs

DELEGATION_ONLY DNSKEY flag

Traditional Key Signing KEY DNSKEY record:

```
powerbind.nohats.ca.  IN DNSKEY 257 3 8 (
         AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
         ) ; KSK; alg = RSASHA256 ; key id = 17869

powerbind.nohats.ca.  IN DS 17869 8 2
f22bbb3315c48b719fb67da0fc019ae4af534143569f7a63022eba4d87c1f56d
```

DNSKEY with DELEGATION_ONLY flag set:

```
powerbind.nohats.ca.  IN DNSKEY 321 3 8 (
         AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
         ) ; KSK; alg = RSASHA256 ; key id = 17933

powerbind.nohats.ca.  IN DS 17933 8 2
096749AAB0CFE225A3779AC7BD21EBDC1D8573511DD5AFA0889EB5E8A00B9AF9
```

Does using a new DNSKEY flag break current deployment? Apparently not!

- powerbind.nohat.ca is a real signed zone using 0x40 DNSKEY flag
- created with a patched dnssec-keygen and dnssec-signzone
  - (ods-ksmutil key import ignored my new dnskey flag)
- So far all tested DNS resolves validate properly
  - Google DNS, bind, powerdns, unbound

Pros

- Protects child zone data from parent
  - Including TLSA, SMIMEA, OPENPGPKEY
- Allows DNSSEC Transparency
- Very simple
  - No new RRTYPE
  - no changes required for authoritative servers
  - Only minimal changes in validator
- Only requires DNS resolver/stub code changes

Cons

- Does not allow exceptions for ENT (“co.uk")
  (no more dots without NS delegations)
- Does not protect child APEX data
  - A/AAAA, MX, IPSECKEY[*]
  - Not a big issue, as we care most about prefixed records, eg TLSA, SMIMEA, DKIM
- Requires delegations for _prefix labels e.g.:
  _tcp.powerbind.nohats.ca. IN NS ...
  _tcp.powerbind.nohats.ca. IN DS ...
  443._tcp.powerbind.nohats.ca. IN TLSA <pubkey>

  (make exception for _prefix labels?)

Deploying DELEGATION_ONLY for the root

- The root zone is *technically* already a delegation only zone. But this is currently not enforced by RFCs or software.
- Is the root *politically* or *legally* a delegation only zone ? Who do we ask? ICANN? IETF ? IANA?
- We can’t realistically set this new flag in time for the September 2018 root KSK rollover. But we don’t want to wait many years for this enhancement to be deployed.
- We could state the root zone is delegation-only even without the DELEGATION_ONLY flag. But once we do, and software implements this, there is no way back

Questions?