

# Why DNSsec?

---

John Crain

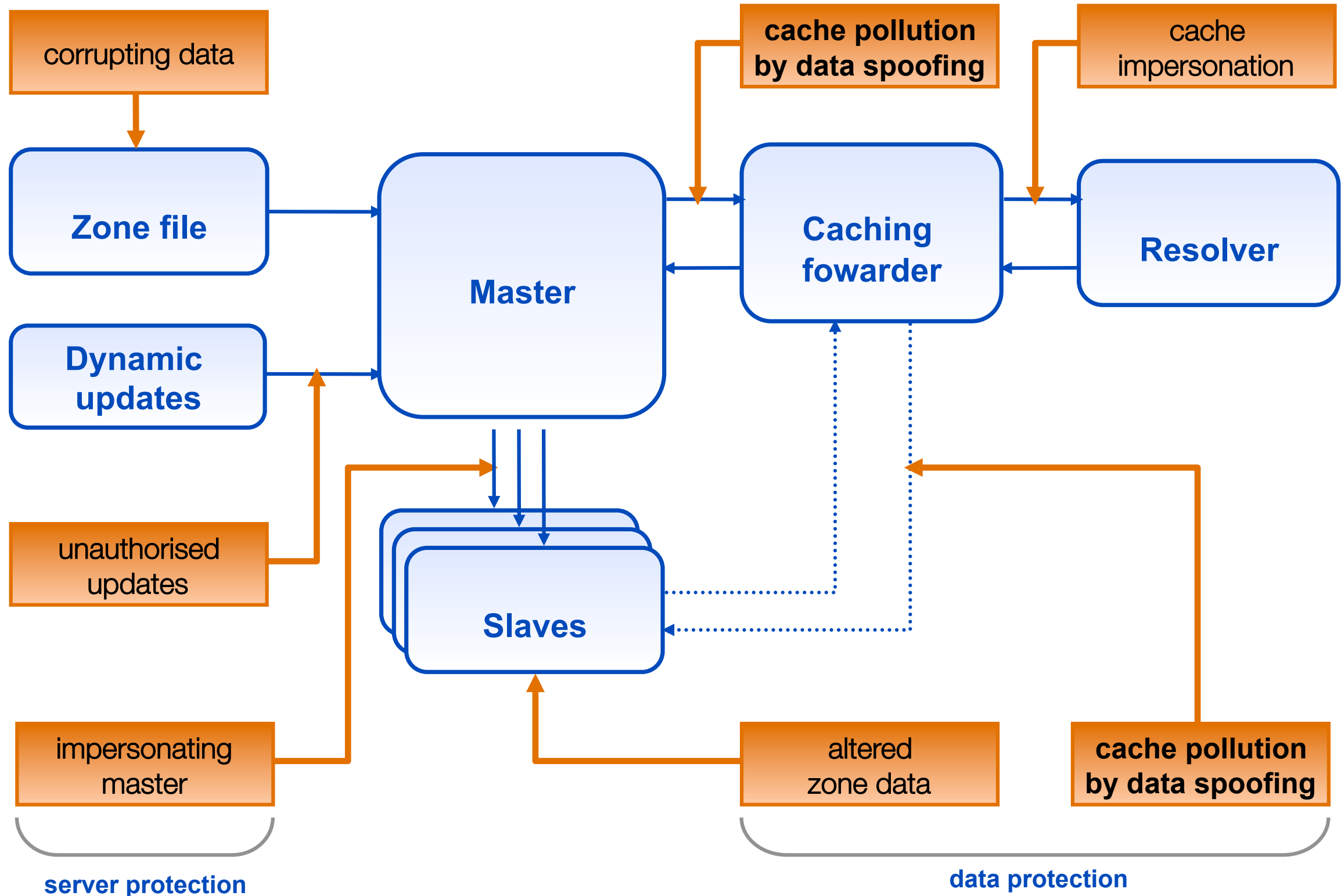
Internet Corporation for Assigned Names and Numbers



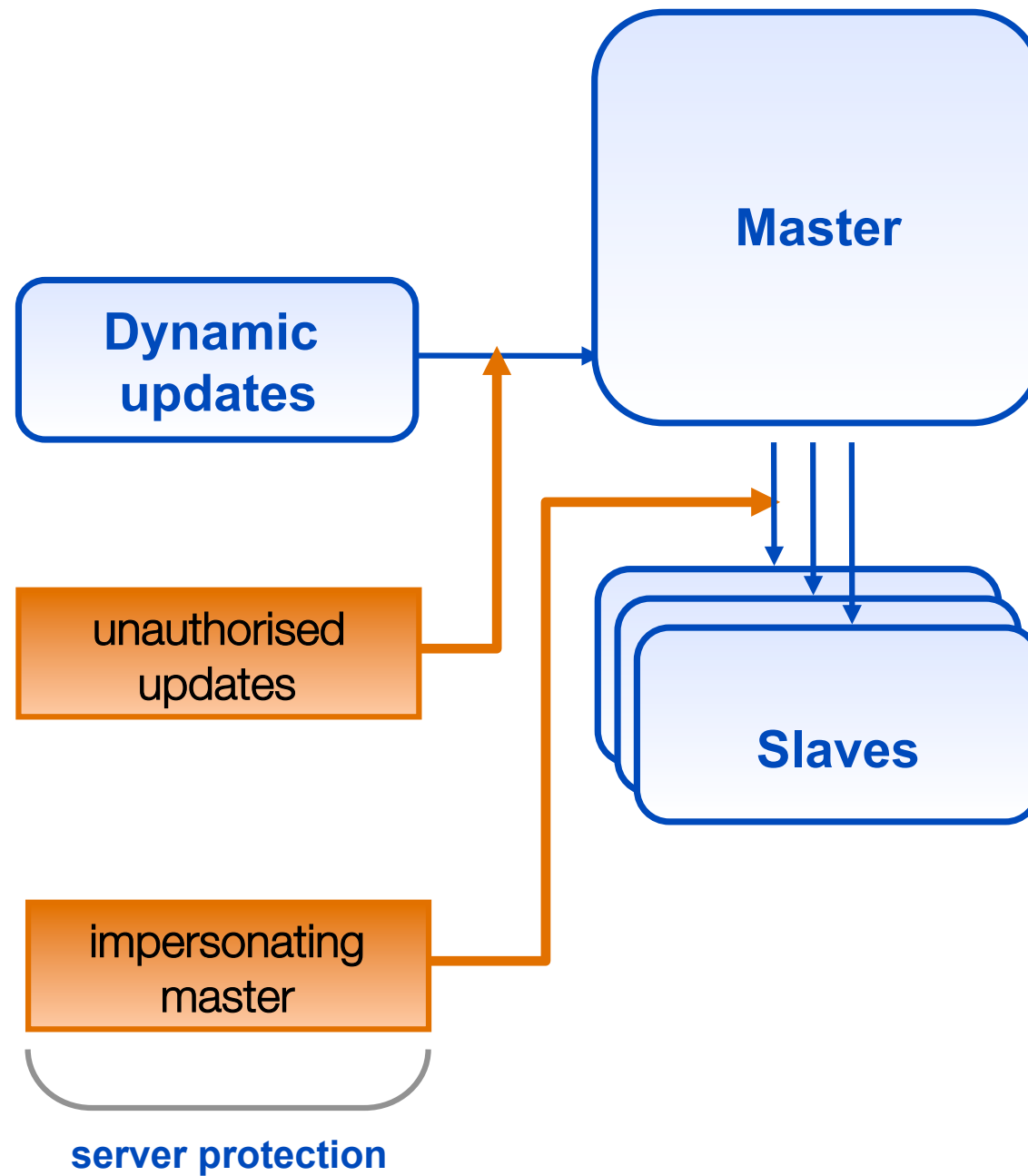
# The DNS is NOT secure

- ▶ When you type [www.icann.org](http://www.icann.org) into a browser you should get a DNS answer of 208.77.188.103
  - ▶ But how do you know that this is the correct answer?
- ▶ Where could it go wrong?

# DNS Vulnerabilities.....



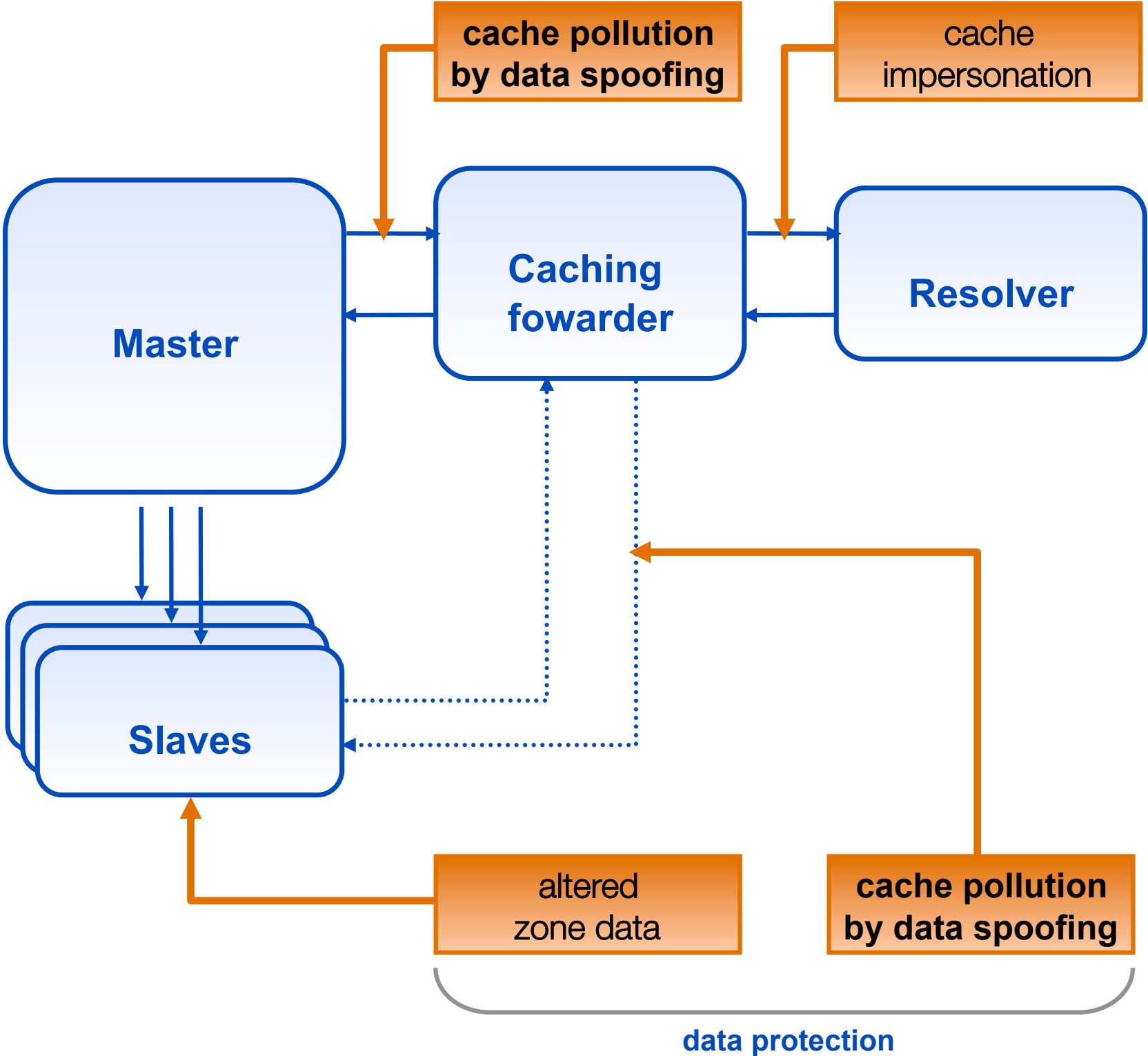
# Server Protection



# Transaction Signatures

- ▶ TSIG = Transaction signature
  - ▶ The master (primary) and slave (secondary) nameservers share a secret to authenticate their identity to each other.
  - ▶ Watch your timing the technique uses time as part of the authentication. If master and slave are >5mins out of synch.. TSIG authentication will fail!

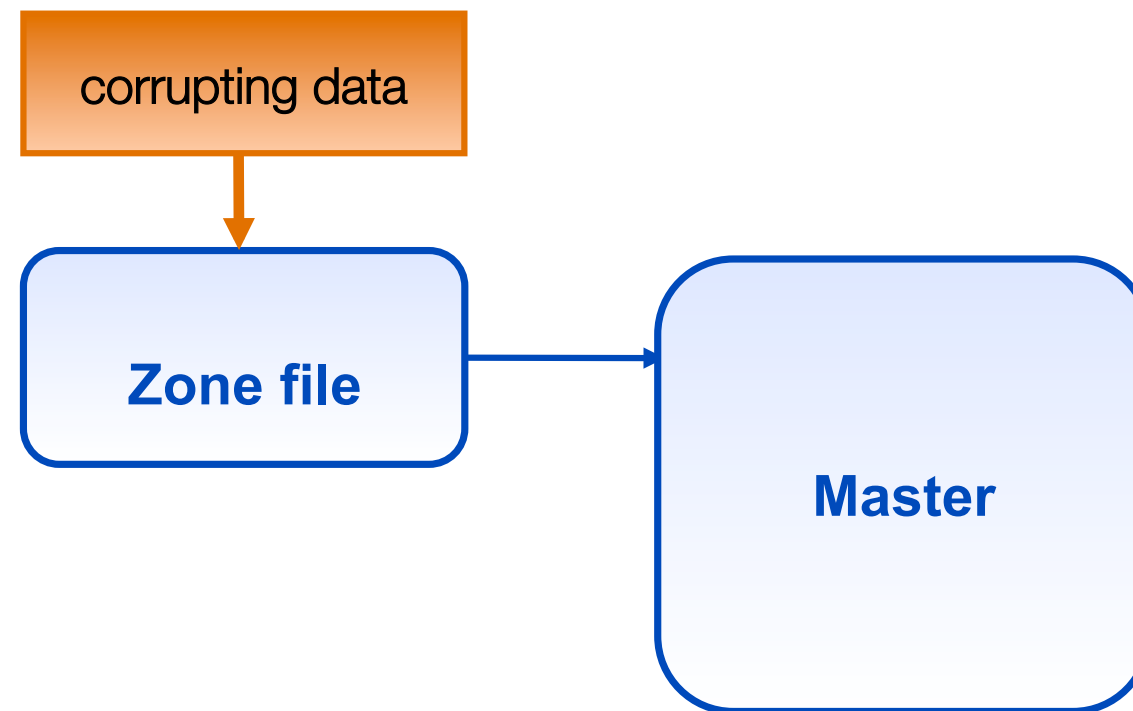
# Data Protection



# Signing the RRsets

- ▶ Use a private key to sign a set of DNS records.
  - ▶ such as
    - ▶ WWW.ICANN.ORG. IN A 208.77.188.103
- ▶ Public key is used to Authenticate the answer
- ▶ This is currently the only way to know that when you ask for www.icann.org you get the authentic answer

# DNSsec is not the cure for all



- ▶ It requires that the original zone file is correct!
- ▶ If someone corrupts the data at the source signing the zone data will not help.



# Things DNSsec does not do

- ▶ DNSsec does NOT provide encryption or any form of privacy
- ▶ DNSsec does not help against DDOS
  - ▶ In fact it could make things worse due to increased CPU usage etc...
- ▶ DNSsec is not the cure for cancer nor will it bring world peace :)
- ▶

# Is anyone using it?

- ▶ TSIG: Is in wide use.
  - ▶ The root zone and many TLD zones use TSIG
- ▶ Signing: Some TLDs and some businesses already use DNSsec.
  - ▶ .gov is about to fully deploy DNSsec
- ▶ The root zone is not yet signed
- ▶ IANA/ICANN has a testbed and technology to do this..
  - ▶ Most of the issues to do with getting the root signed are now at “Layer 9” that’s tech talk for the Political Layer

# Some Resources

- ▶ <http://www.dnssec.net>
- ▶ <http://www.bind9.net>
- ▶ <http://www.dnsreport.com>
- ▶ <http://www.dnssec-deployment.org/>

# Thankyou for your attention!

---

John Crain  
[john.crain@icann.org](mailto:john.crain@icann.org)

