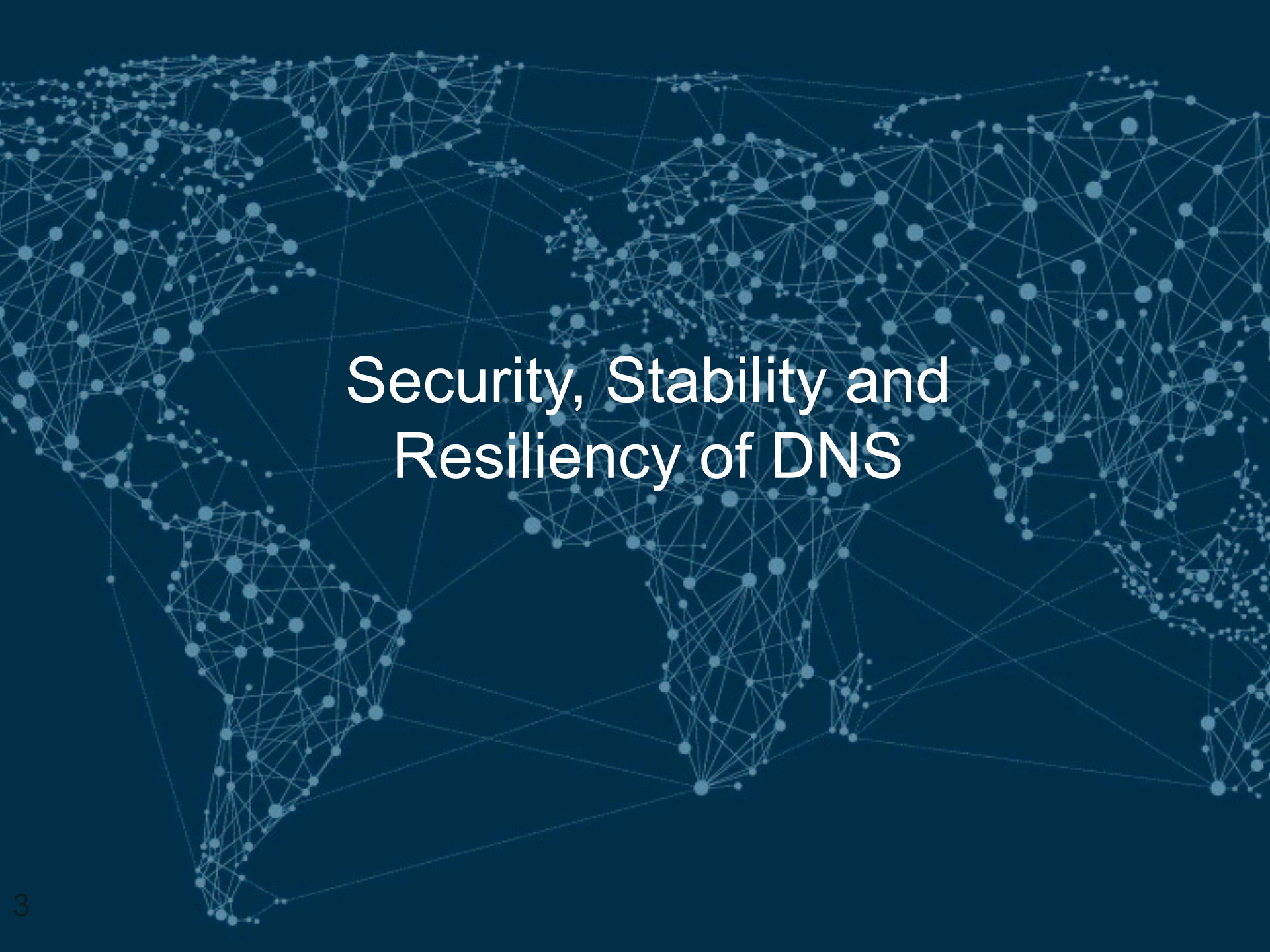
DNS and ccTLD Management

Save Vocea and Champika Wijayatunga | Apia – Samoa | 14-15 July 2015

Agenda

1. Intro to ICANN
2. DNS Concepts
3. Root Server Operation
4. Managing Zones
5. ccTLD Management
6. Security, Stability and Resiliency of DNS


Security, Stability and
Resiliency of DNS

+1-202-7
VoIP

HealthCare.gov

US-NSTIC effort

Google

OpenID

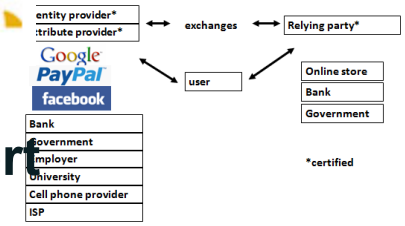
DNS is a part of all IT ecos s

facebook

ebay

AADHAAR

PayPal

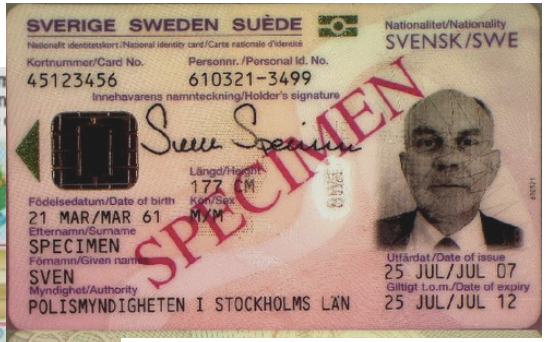


OECS ID effort

amazon Prime

e-Passport symbol

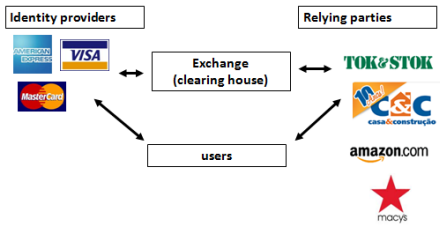
ICP Brasil
O Brasil na era da certificação digital



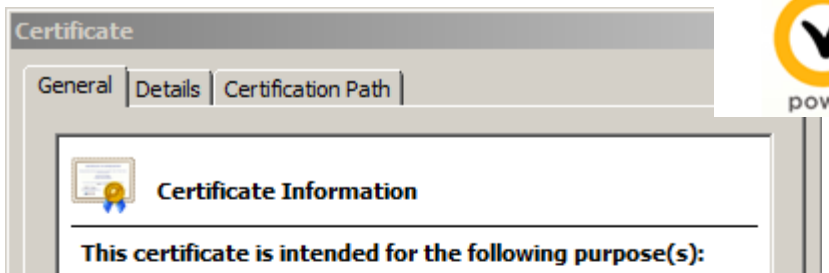
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

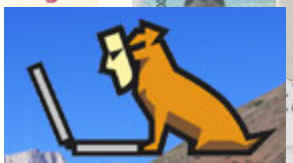
Trust frameworks are not new



Smart Electrical Grid



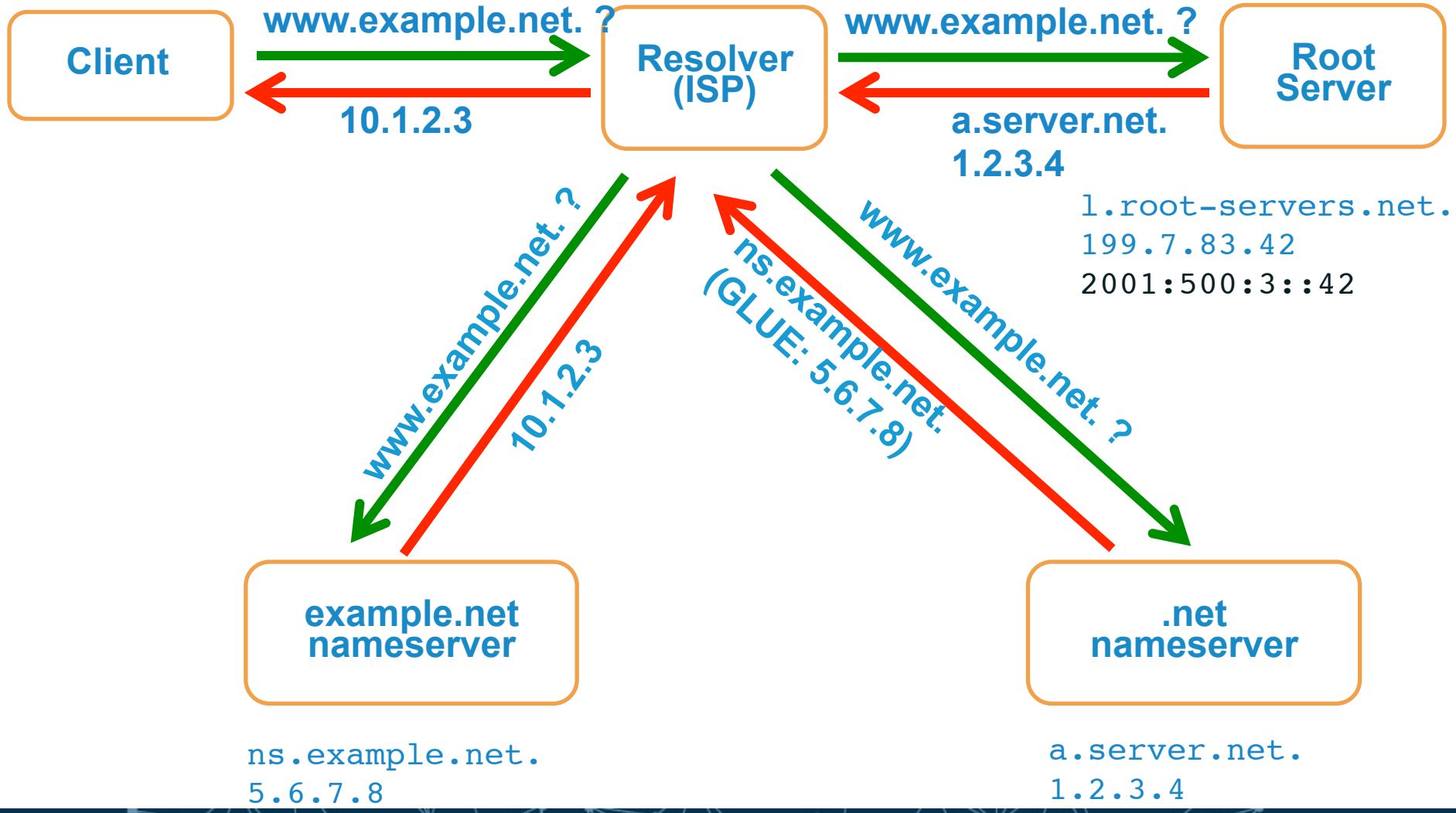
Norton SECURED
powered by VeriSign



lamb@xtcn.co
m

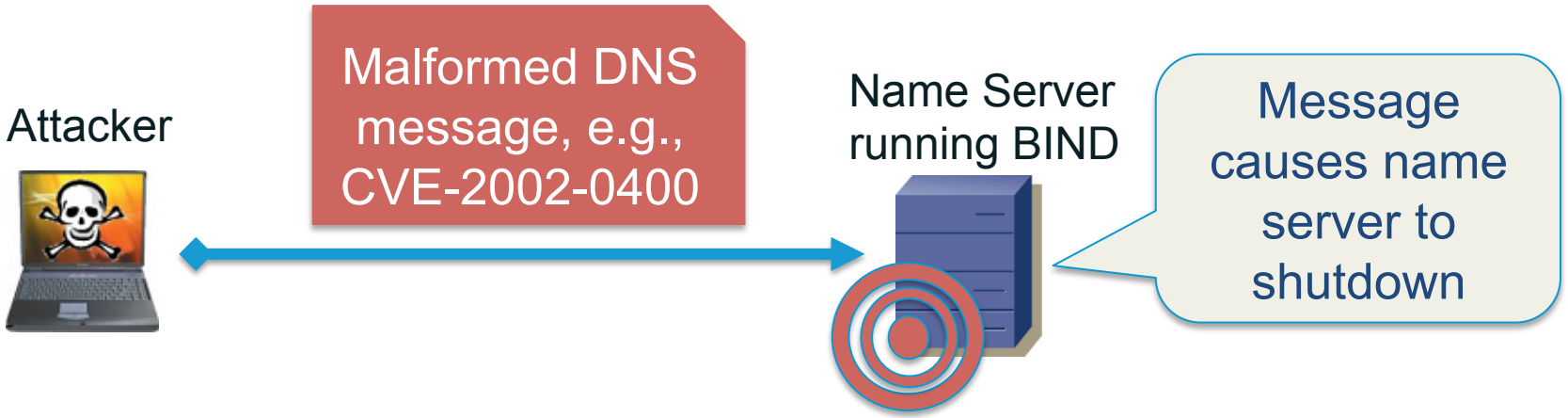
mydomainname.co

DNS Resolution



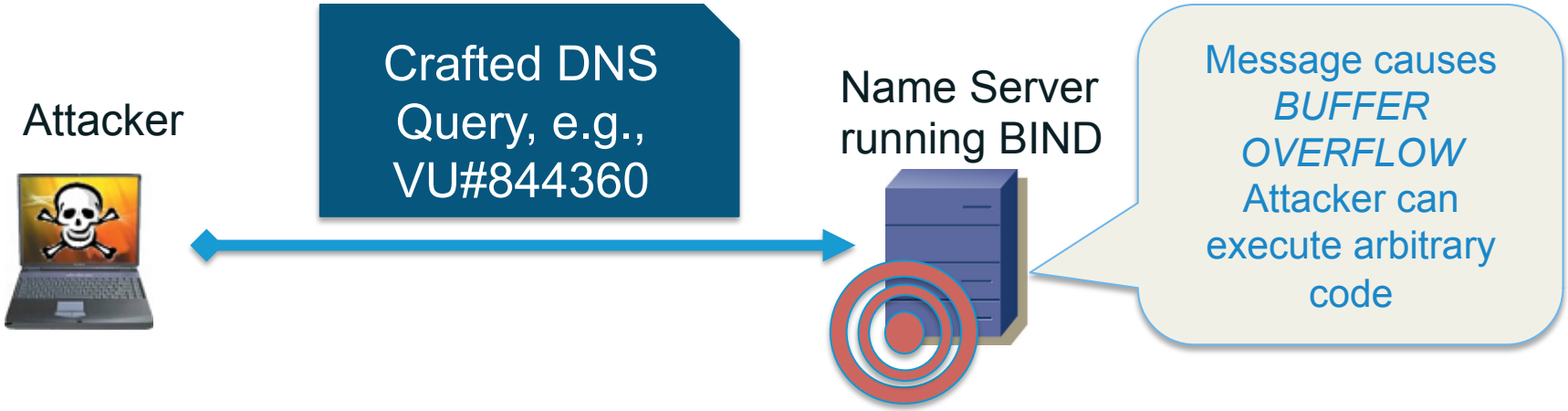
“Exploit to fail” DOS attack

- Exploit a vulnerability in some element of a name server infrastructure to cause interruption of name resolution service
- Example: Malicious DNS message injection
  - http://www.cvedetails.com/cve/CVE-2002-0400/

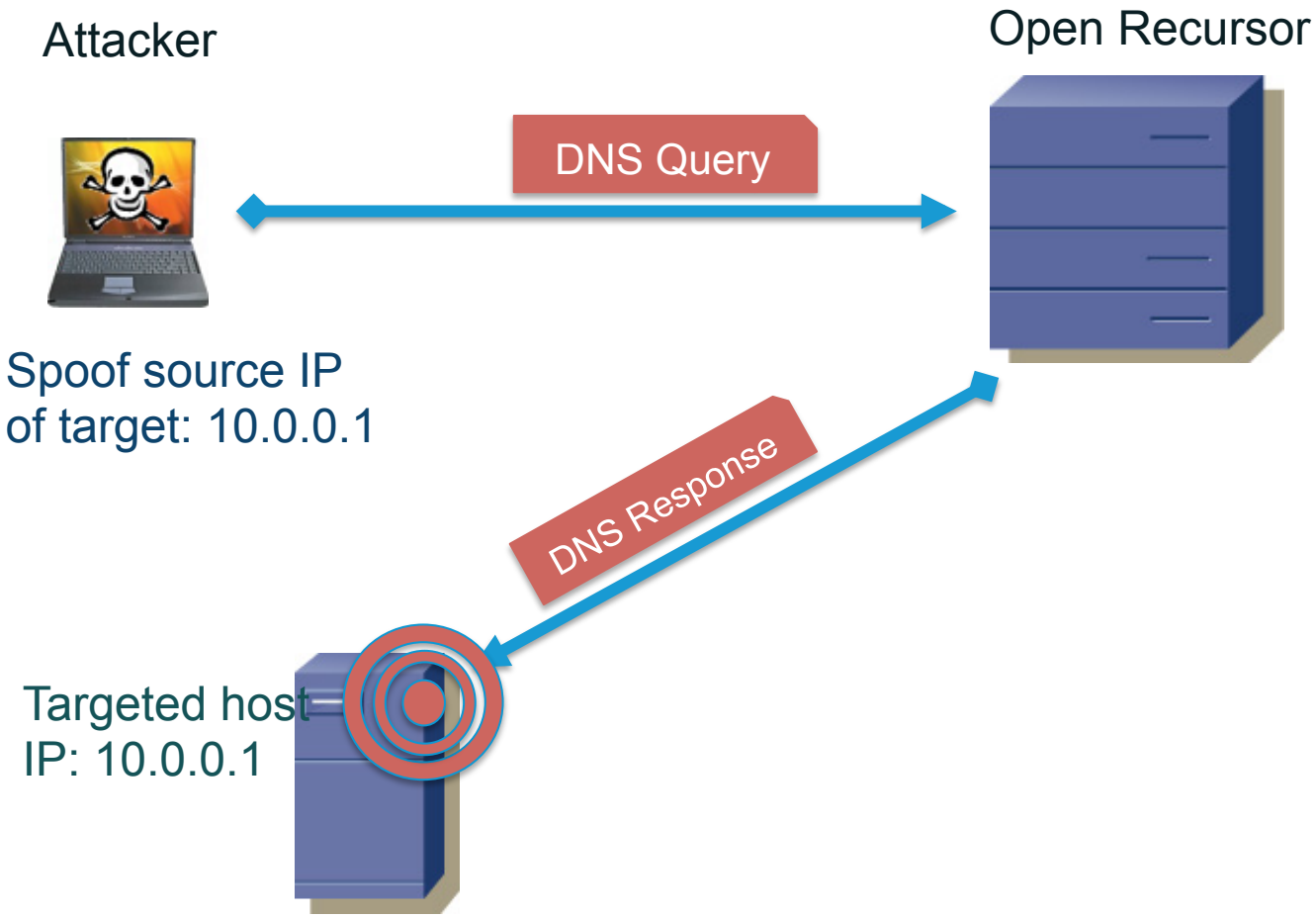


“Exploit to own” DOS attack

- Exploit a vulnerability in some element of a name server infrastructure to gain system administrative privileges
- Example: Arbitrary/remote code execution
  - http://www.kb.cert.org/vuls/id/844360

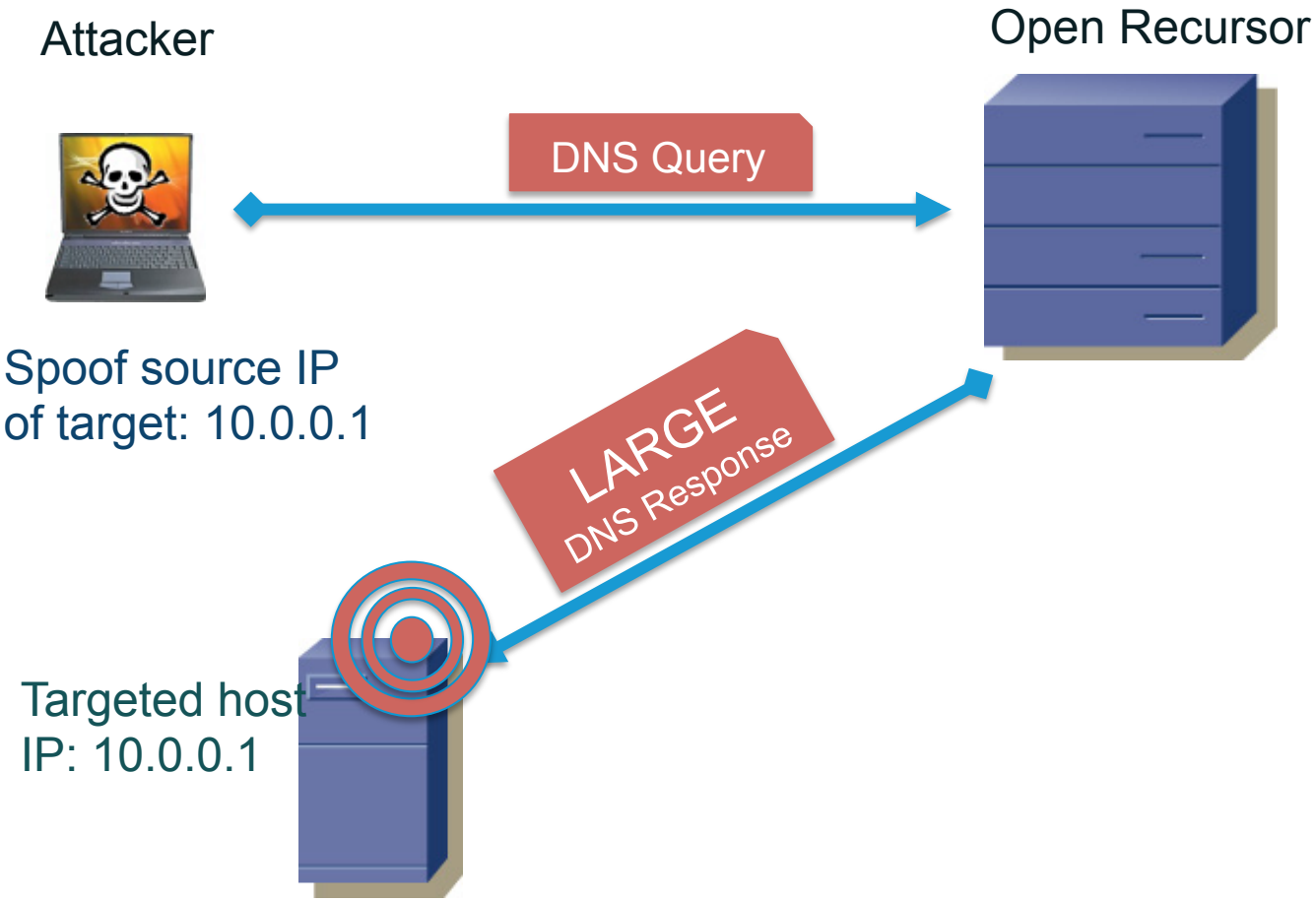


Reflection attack



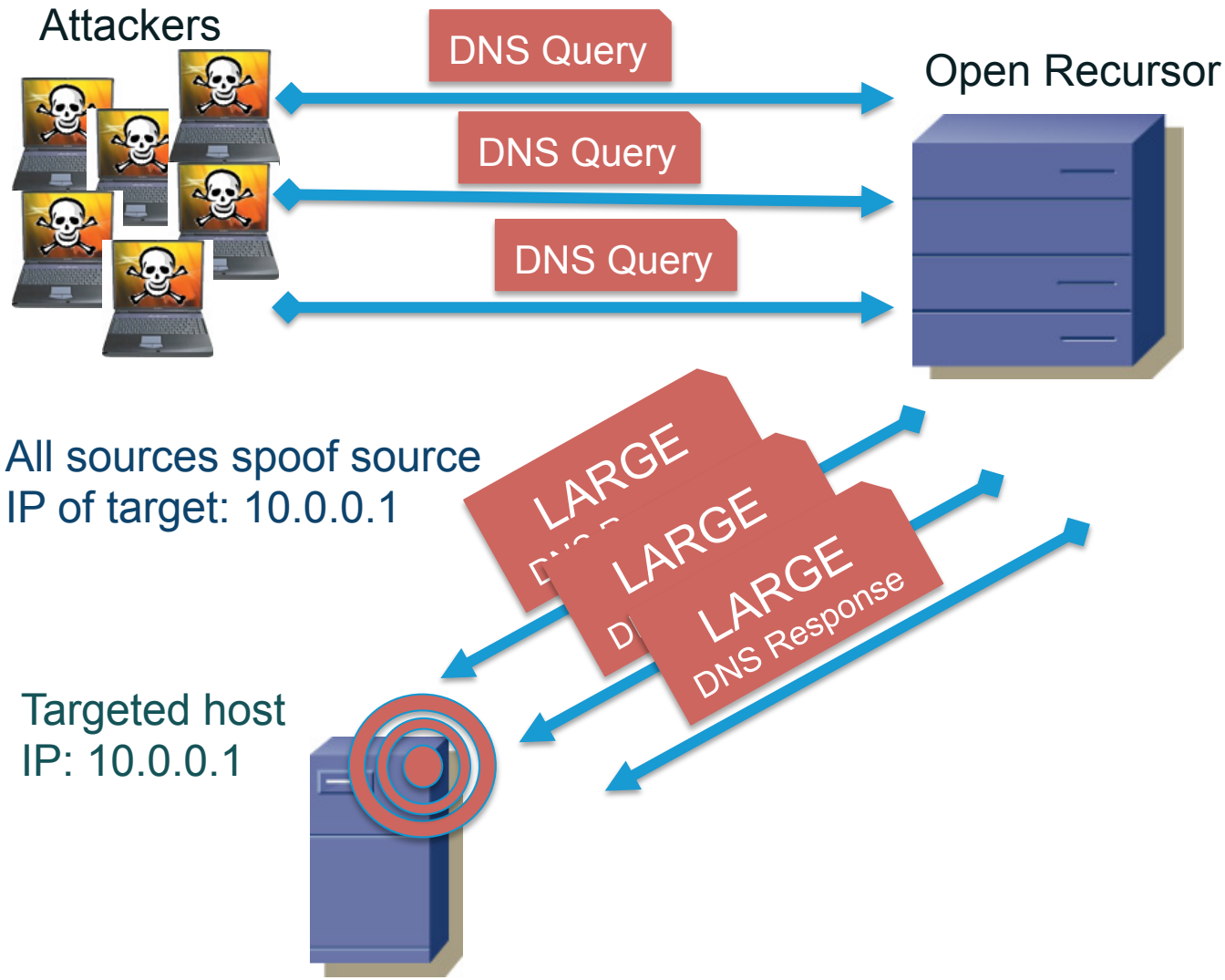
- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends response to targeted host
- Response delivered to targeted host

Reflection and Amplification attack



- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends LARGE responses to targeted host
- *Amplified* responses delivered to targeted host consume resources faster

Distributed reflection and amplification attack (DDoS)



- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

Basic Cache Poisoning

Attacker

- Launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

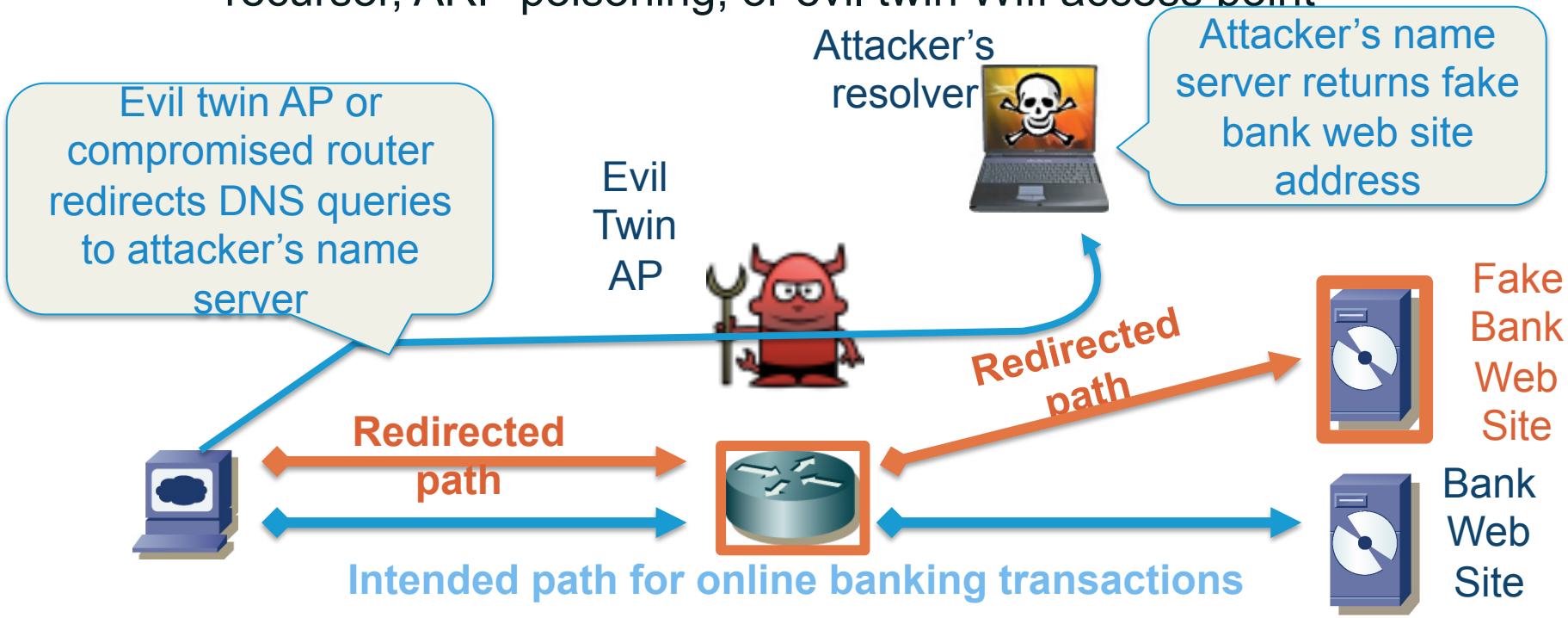
Reconnaissance Attacks

- Zone Transfer
  - Impersonate a secondary name server
  - Ask primary for zone
- Zone Enumeration, a.k.a.,
  - “zone walk”
  - Use a “dictionary” of subdomain labels to get partial name space and topology information

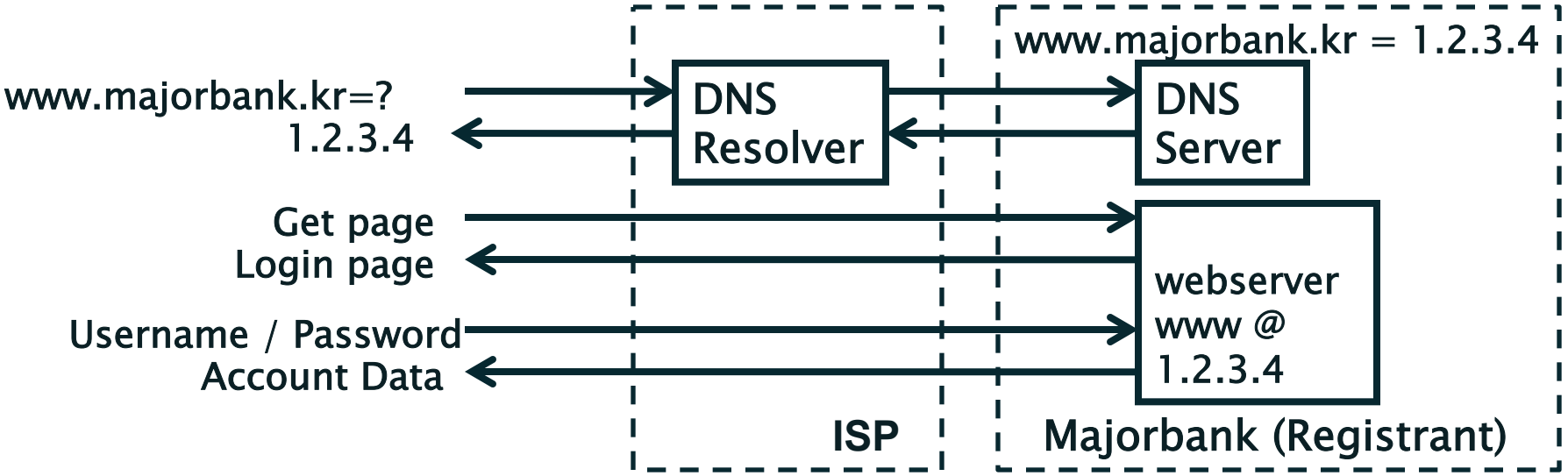
These precursor attacks provide intelligence for subsequent attacks

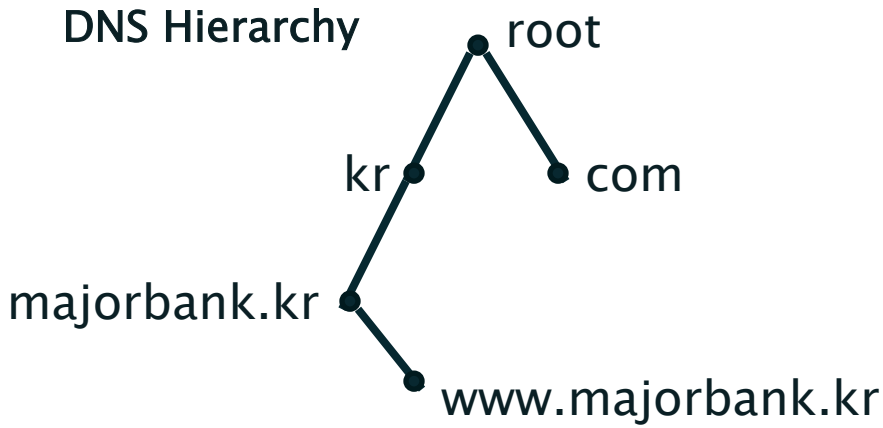
Query Interception (DNS Hijacking)

- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point

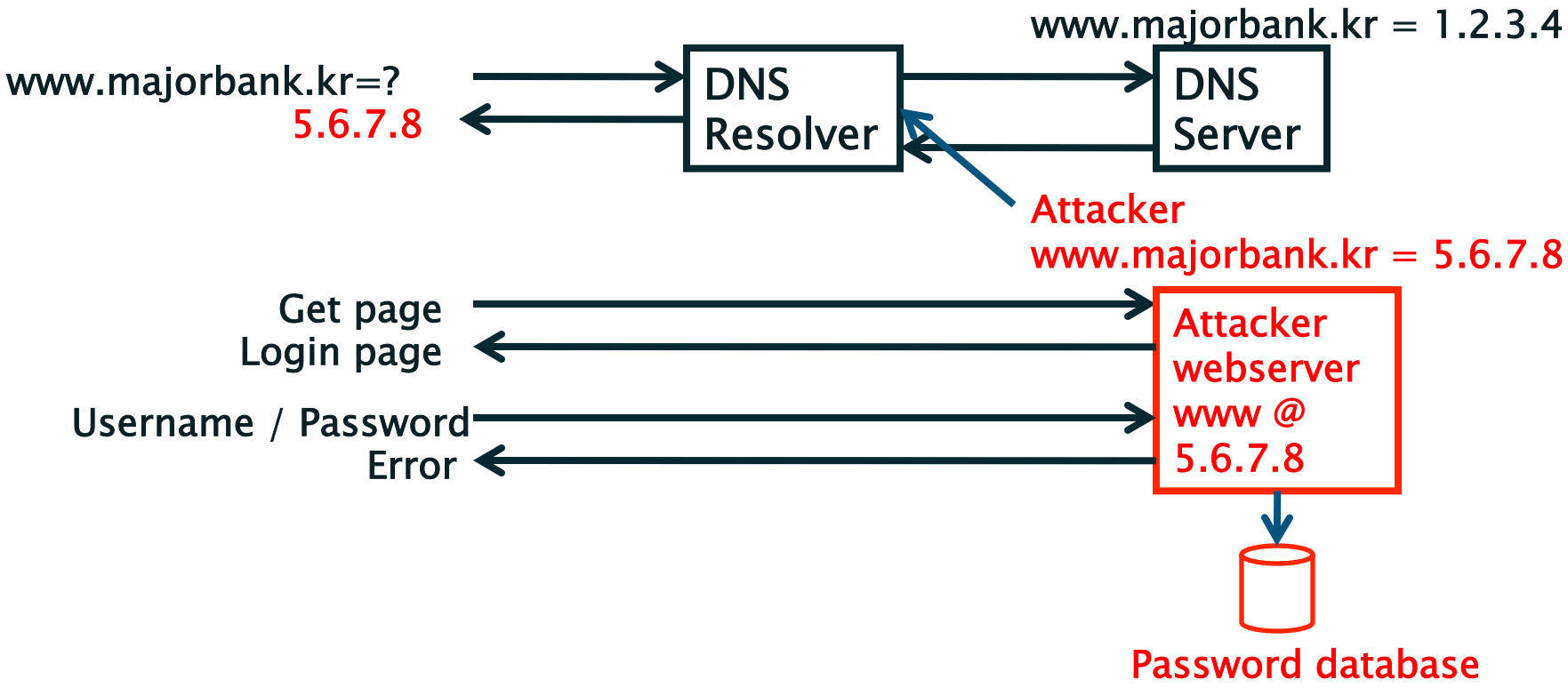


The Internet's Phone Book - Domain Name System

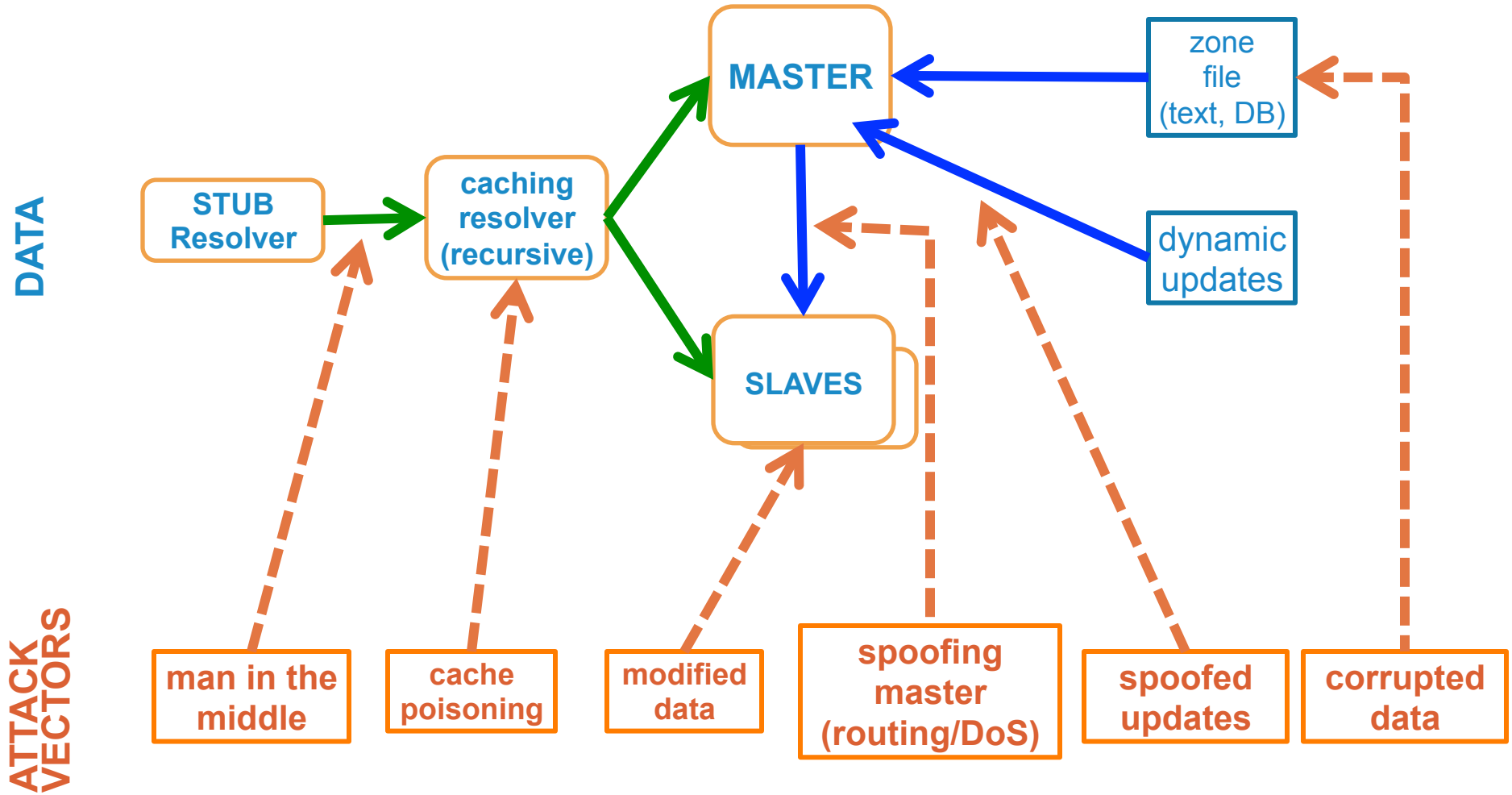




The Problem: DNS Cache Poisoning Attack



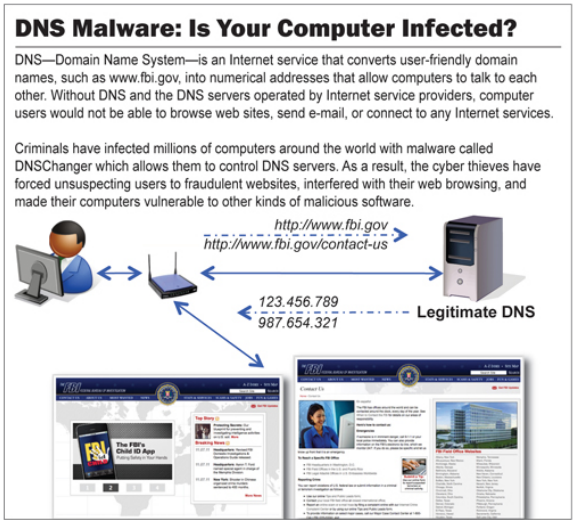
DNS Data Flow



The Bad

- DNSChanger*
  - Biggest Cybercriminal Takedown in History
  - 4M machines, 100 countries, $14M

- And many other DNS hijacks in recent times**

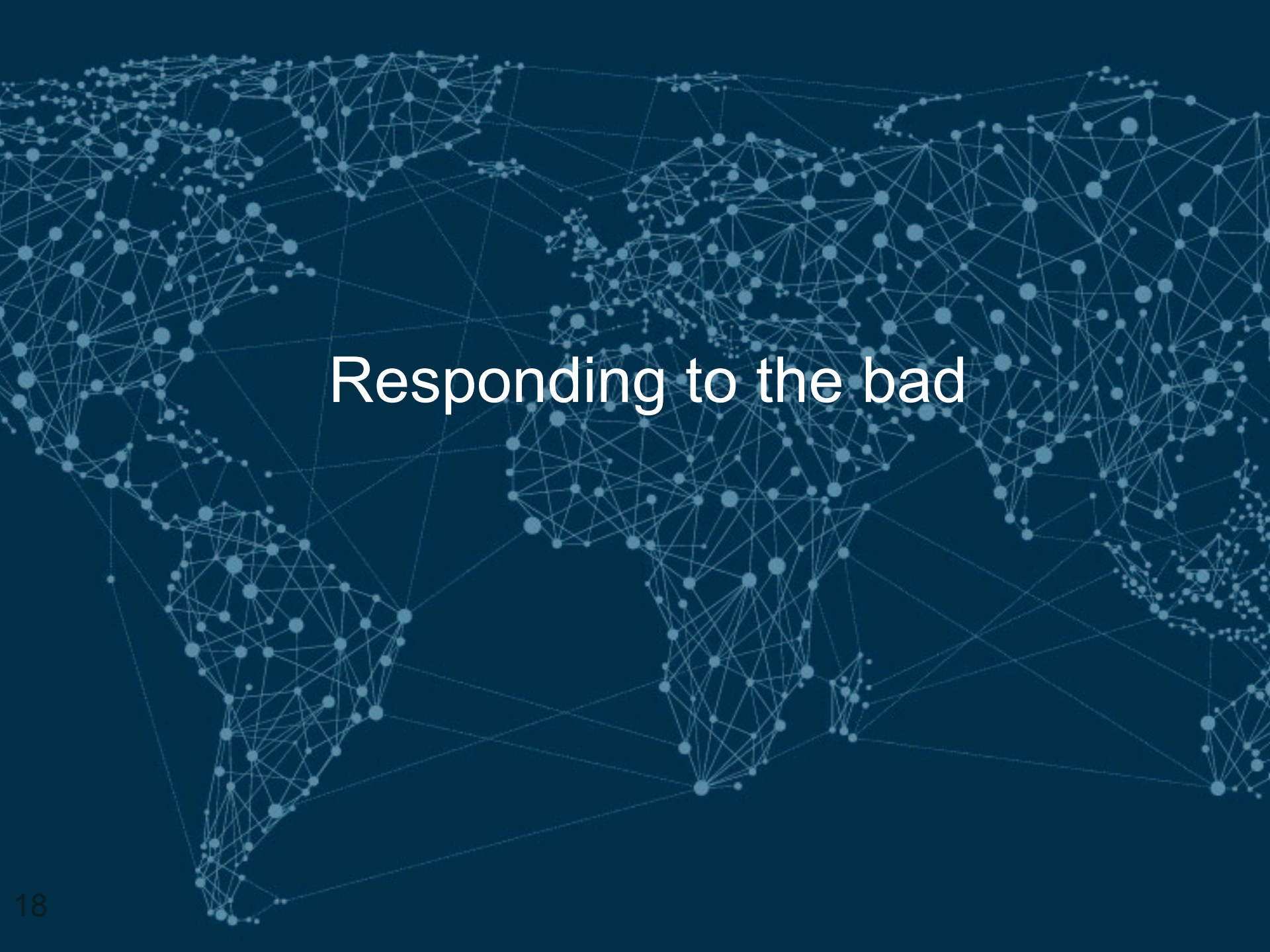


- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

DigiNotar® A VASCO COMPANY

* **http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911**
End-2-end DNSSEC validation would have avoided the problems

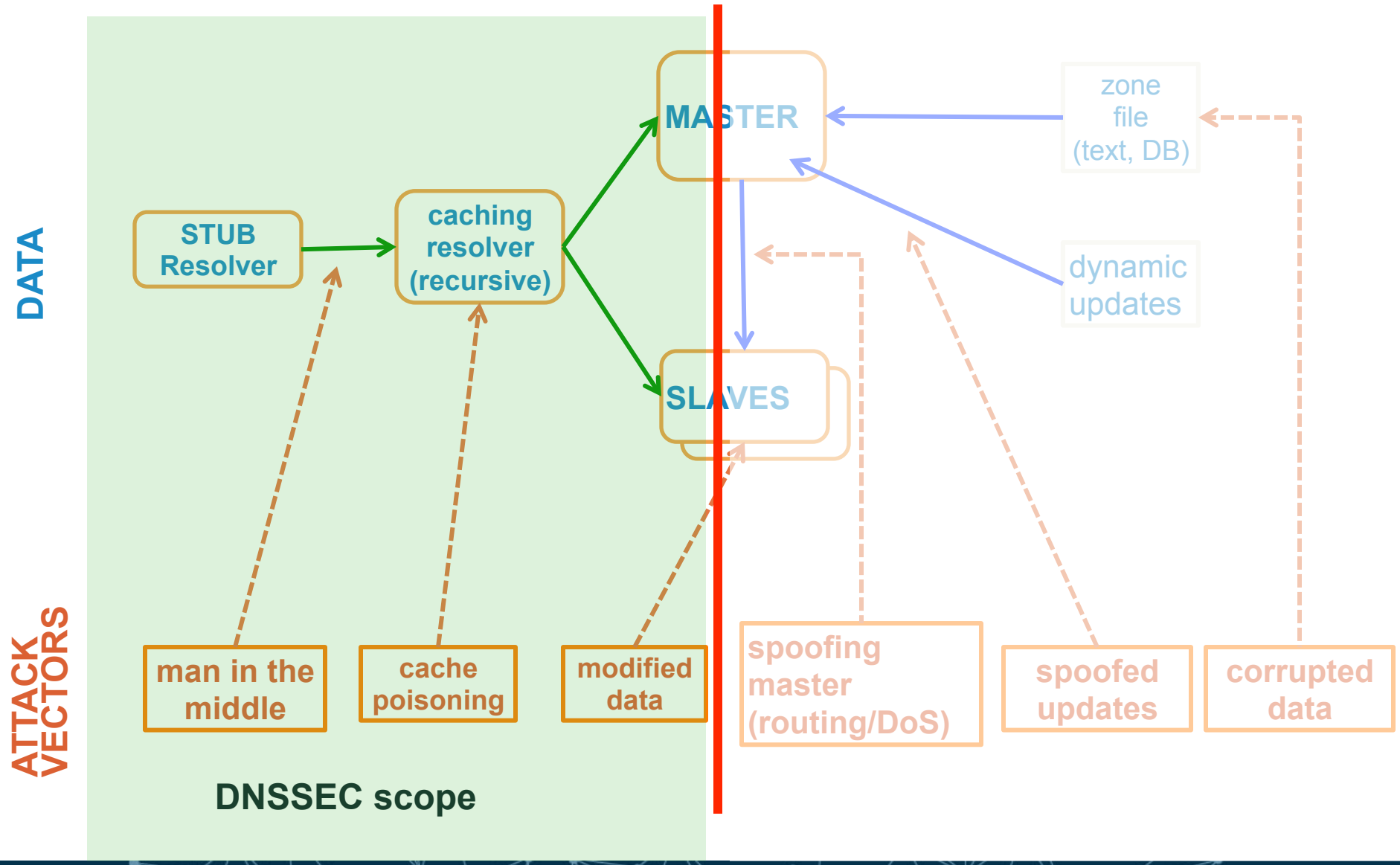
** **A Brief History of DNS Hijacking - Google**
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf


Responding to the bad

Where DNSSEC fits in

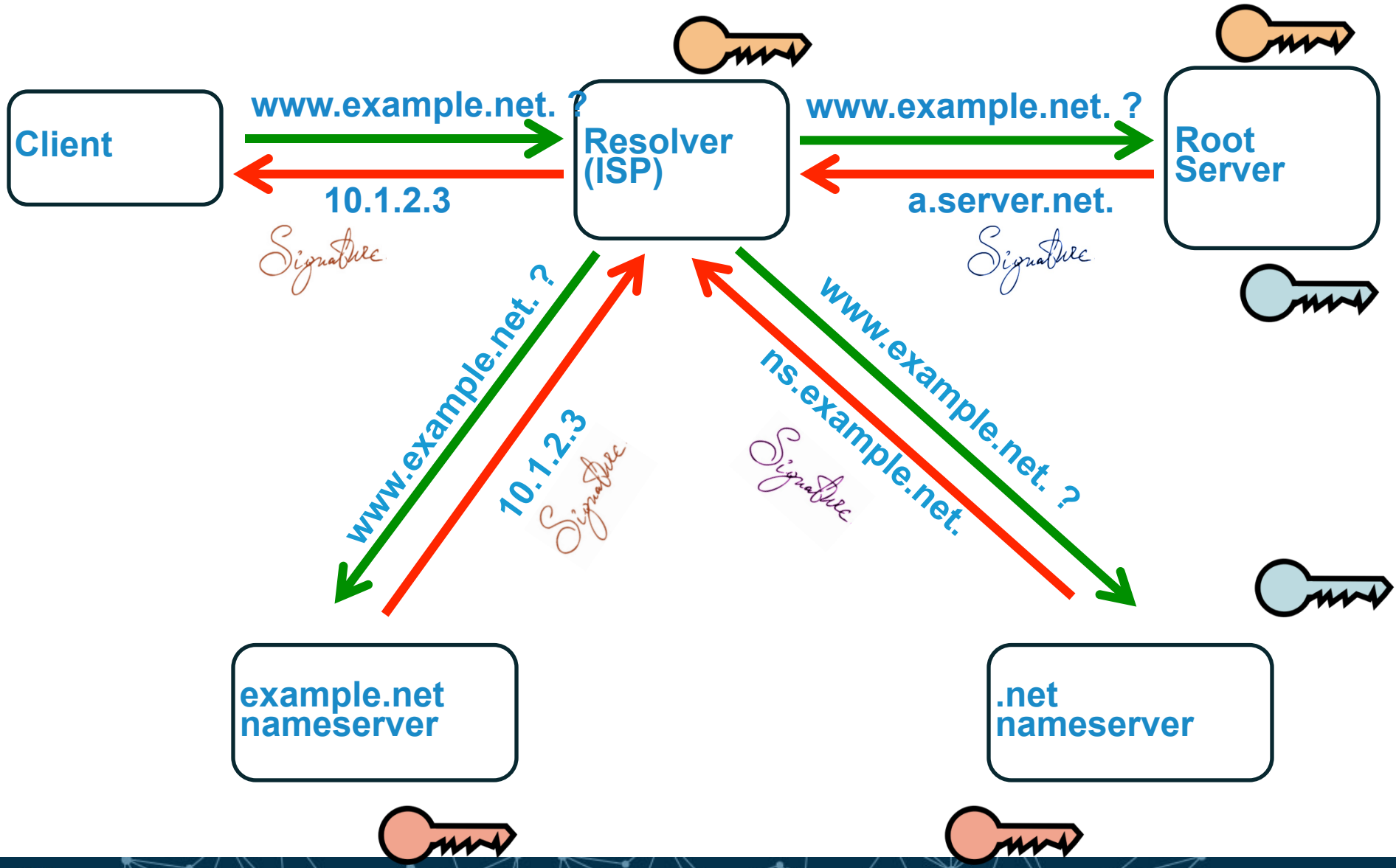
- CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
- DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents
- With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)

What DNSSEC solves




How DNSSEC Works?

How DNSSEC Works



How DNSSEC Works

- Data authenticity and integrity by signing the Resource Records Sets with a private key
- Public DNSKEYs published, used to verify the RRSIGs
- Children sign their zones with their private key
  - Authenticity of that key established by parent signing hash (DS) of the child zone's key
- Repeat for parent…
- Not that difficult on paper
  - Operationally, it is a bit more complicated
  - $DS_{KEY} \rightarrow$ KEY –signs→ zone data

The Business Case for DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.

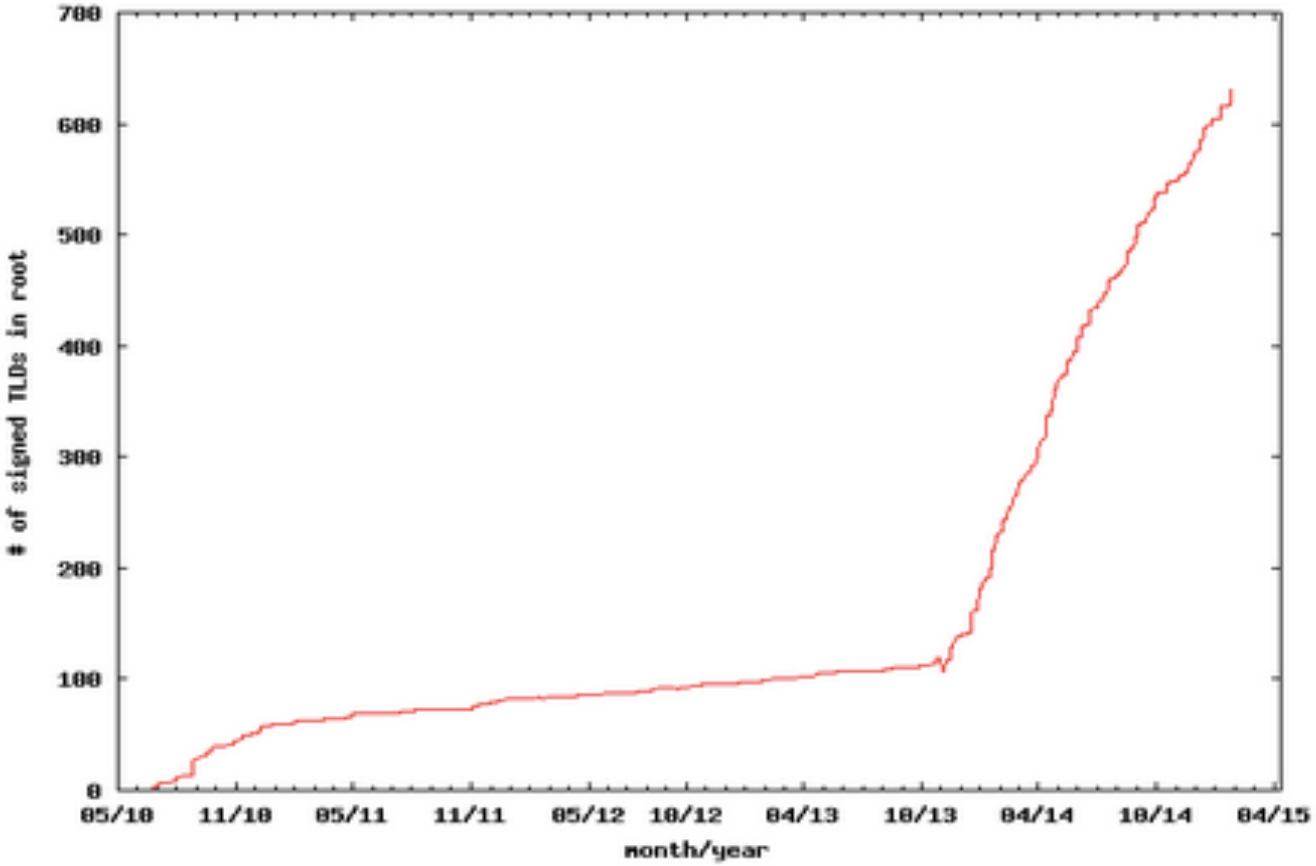
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

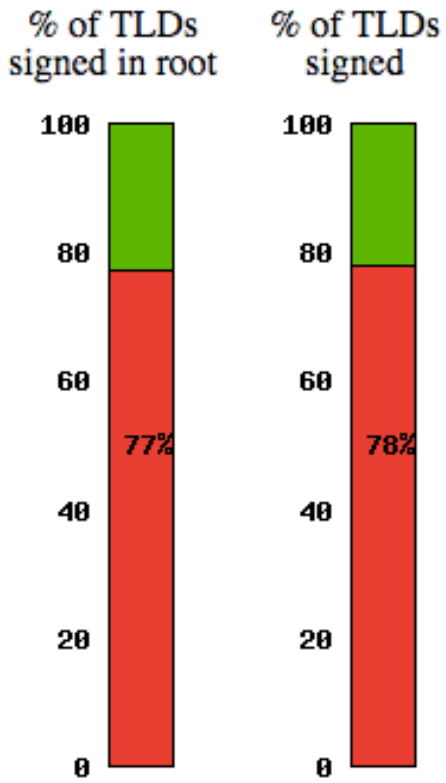
- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC ccTLD Map

https://rick.eng.br/dnssecstat/

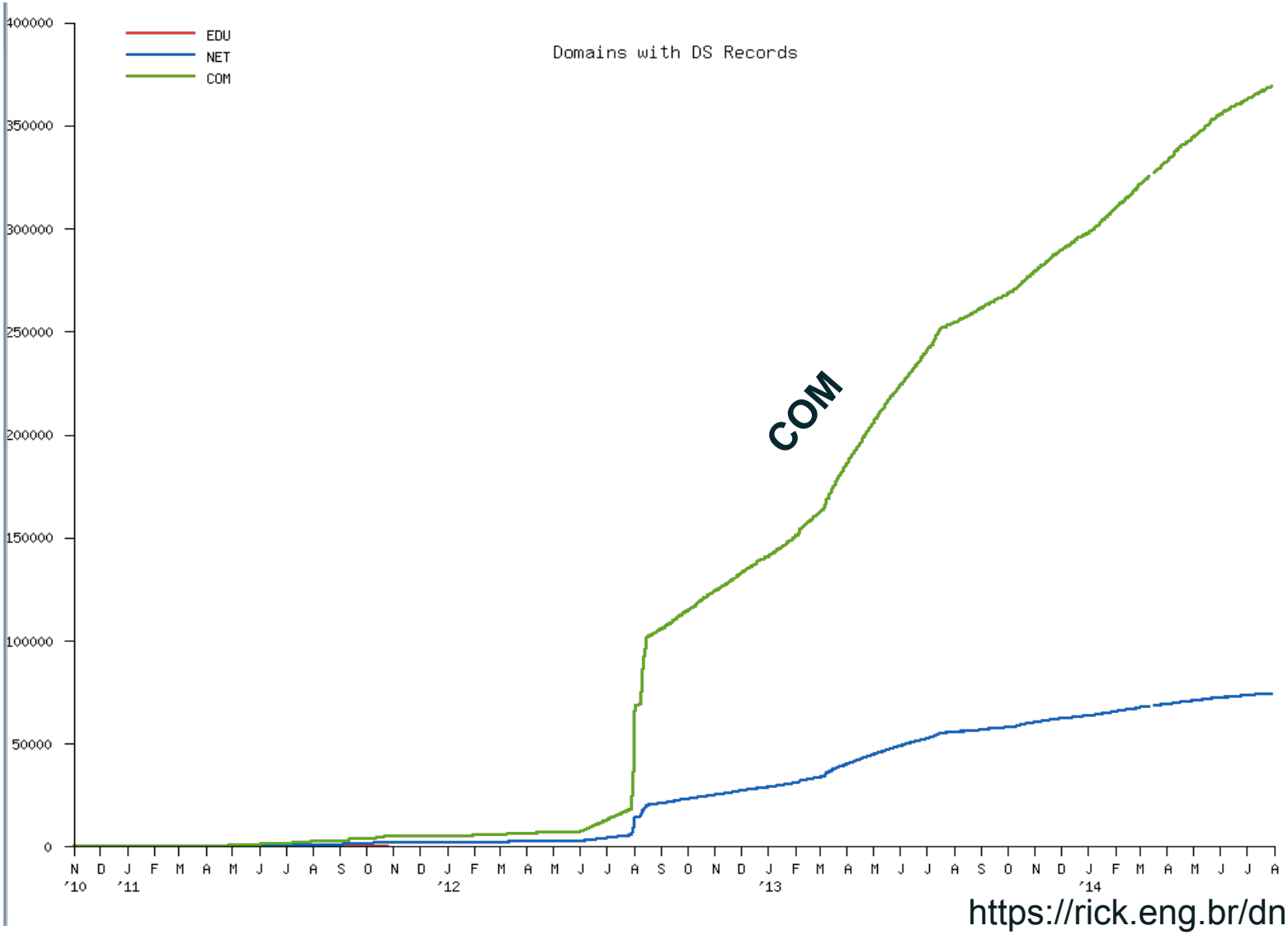
DNSSEC TLDs





https://rick.eng.br/dnssecstat/

Domains with DS records



https://rick.eng.br/dnssecstat/

DNSSEC - Where we are

- Deployed on 805/982 TLDs (25 Jun 2015 82% .com .hr .es .in .af .ee .lb .bg .tm .cz .nl .uk .de .jp .cn .ru . pф .my ملیسیا .asia .tw 台灣, .kr 한국 .net, .org, .post, +gtlds)
- Root signed** and audited
- Required in new gTLDs. Basic support by ICANN registrars
- Growing ISP support*.
- 3rd party signing solutions***
- Growing S/W H/W support: NLNetLabs, ISC, Microsoft, PowerDNS, Secure64…openssl, postfix, XMPP, mozilla: early DANE support
- IETF standard on DNSSEC SSL certificates (RFC6698)
- Growing support from major players…(Apple iPhone/iPad, Google 8.8.8.8,…)

*** COMCAST /w 20M and others; most ISPs in SE ,CZ. AND ~12% of resolvers validate using DNSSEC**

****Int'l bottom-up trust model /w 21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ…**

***** Partial list of registrars: https://www.icann.org/en/news/in-focus/dnssec/deployment**

But…

- DNSSEC Validation for World is ~ 13.68%
- Many 2nd level domains have plans. Some have taken the step (e.g., yandex.com, paypal.com*, comcast.com).
- DNSChanger and other attacks highlight today's need. (e.g end-2-end DNSSEC validation would have avoided the problems)
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.

http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=1&w=7&g=0
http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html

DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.

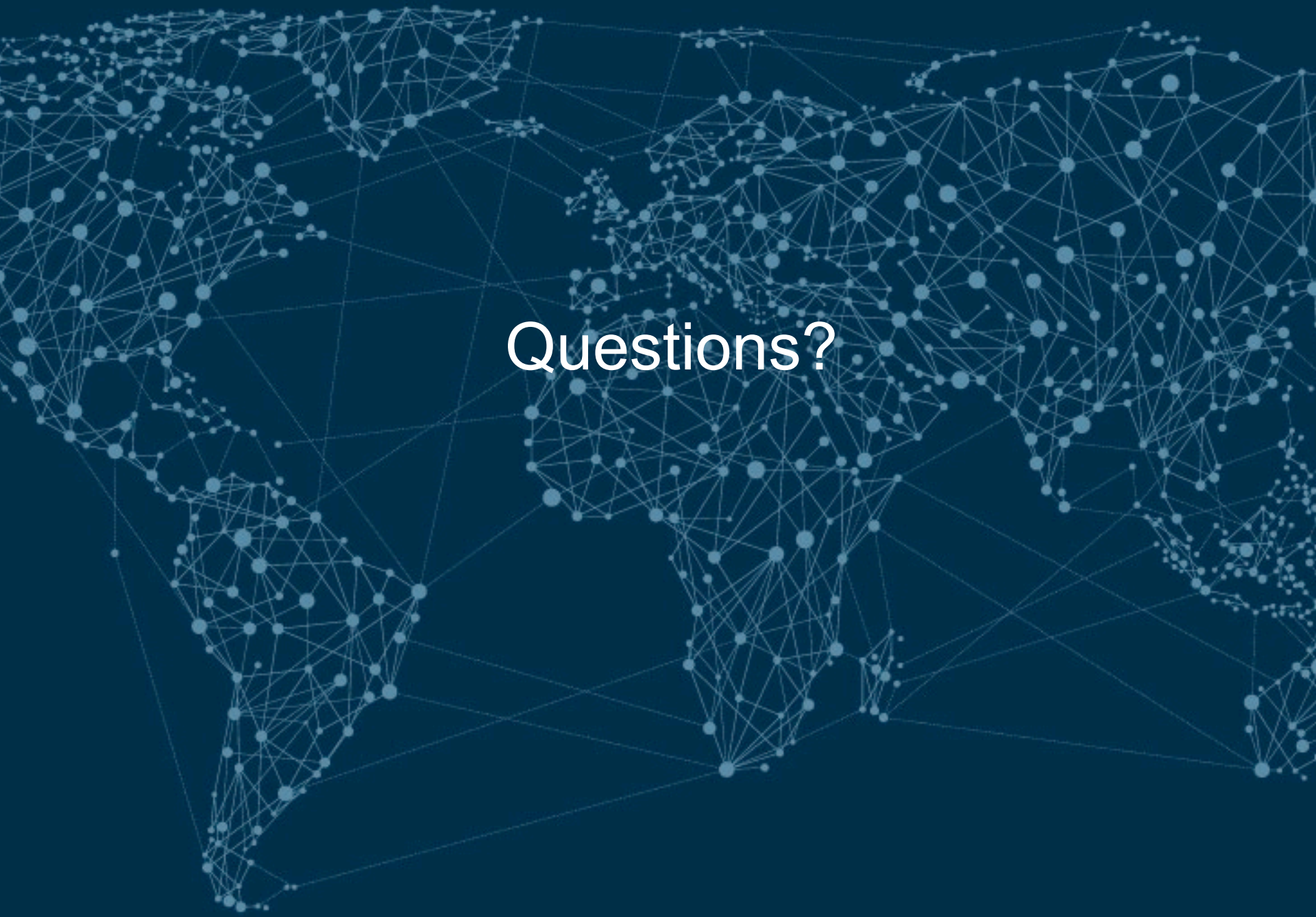
*but required by new ICANN registrar agreement

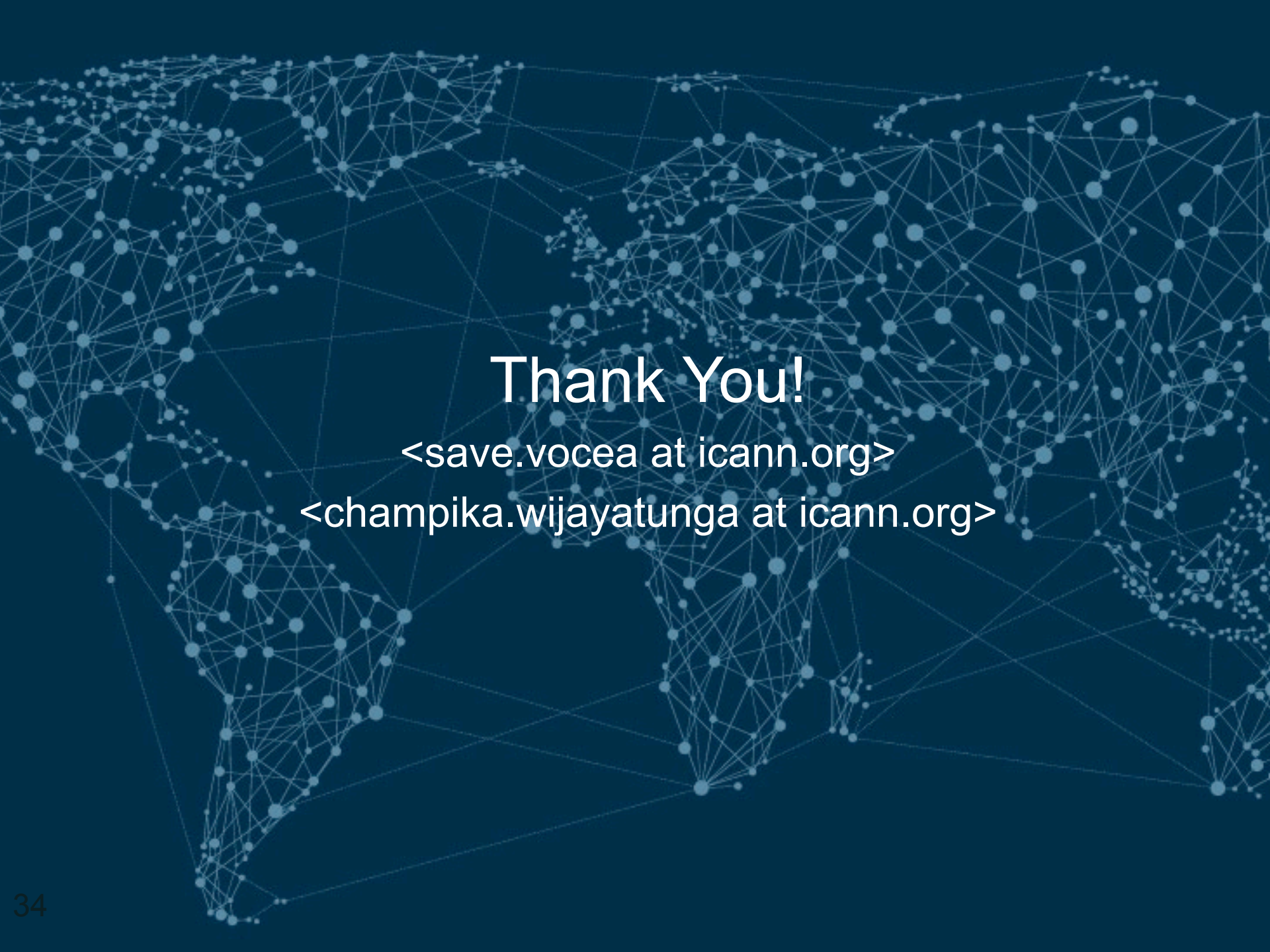
What you can do

- ***For Companies:***
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- ***For Users:***
  - Ask ISP to turn on validation on their DNS resolvers
- ***For All:***
  - Take advantage of DNS / DNSSEC education and training

Summary

1. Intro to ICANN
2. DNS Concepts
3. Root Server Operation
4. Managing Zones
5. ccTLD Management
6. Security, Stability and Resiliency of DNS


Questions?


Thank You!
<save.vocea at icann.org>
<champika.wijayatunga at icann.org>