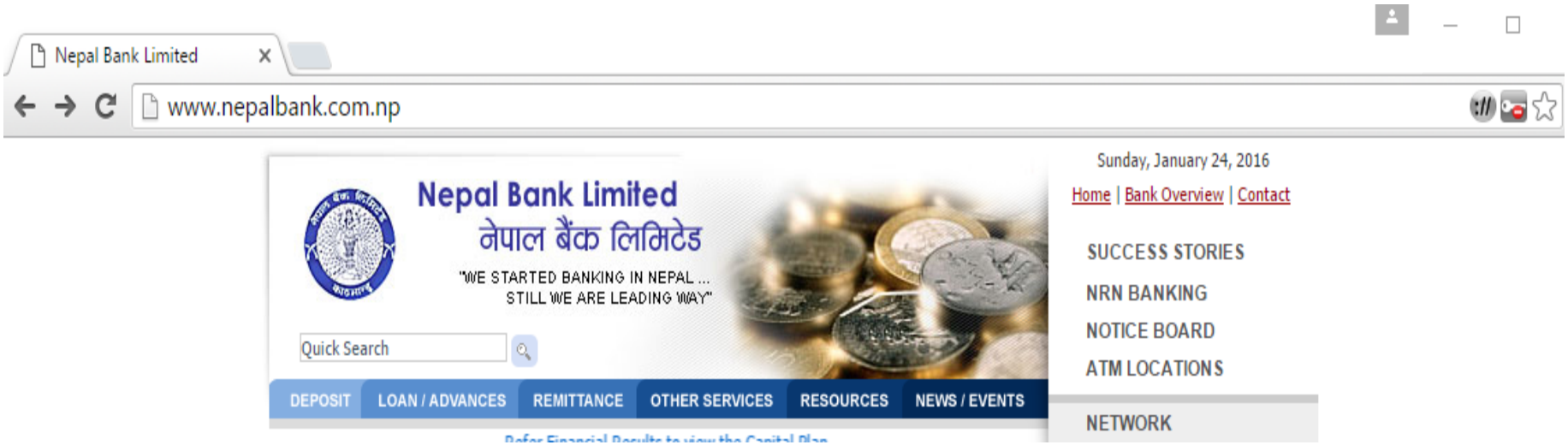
DNSSEC Update

SANOG 27
Kathmandu, Nepal
January 2016
Richard.Lamb@icann.org

DNS Basics

- DNS converts names (www.nepalbank.com.np) to numbers (198.1.112.132)
- ..to identify services such as www and e-mail
- ..that identify and link customers to business and visa versa



+1-202-709-5262 VoIP

HealthCare.gov

US-NSTIC effort

DNS is a part of all IT ecosystems (much more than one expects)

Google

OpenID

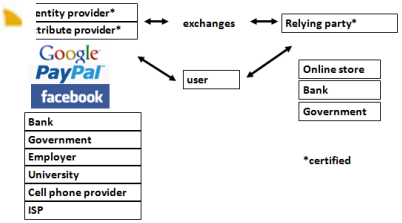
facebook

ebay

AADHAAR

PayPal

OECS ID effort



amazon Prime

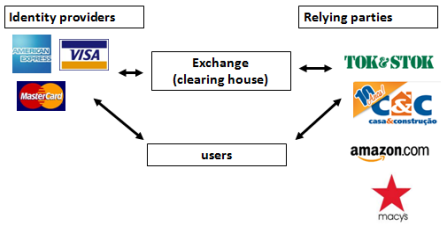
e-Passport symbol

ICP Brasil
O Brasil na era da certificação digital

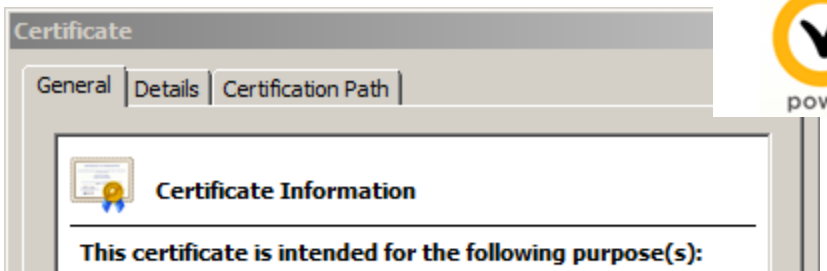
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

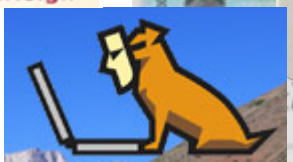
Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign



lamb@xtcn.com

mydomainname.com

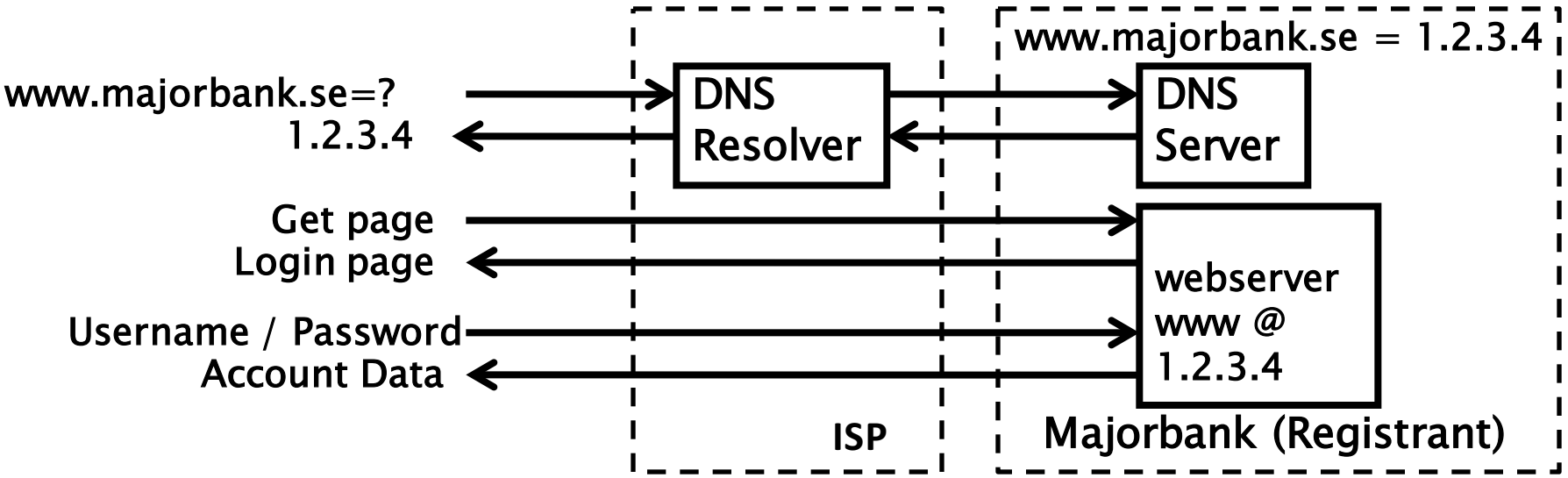
Where DNSSEC fits in

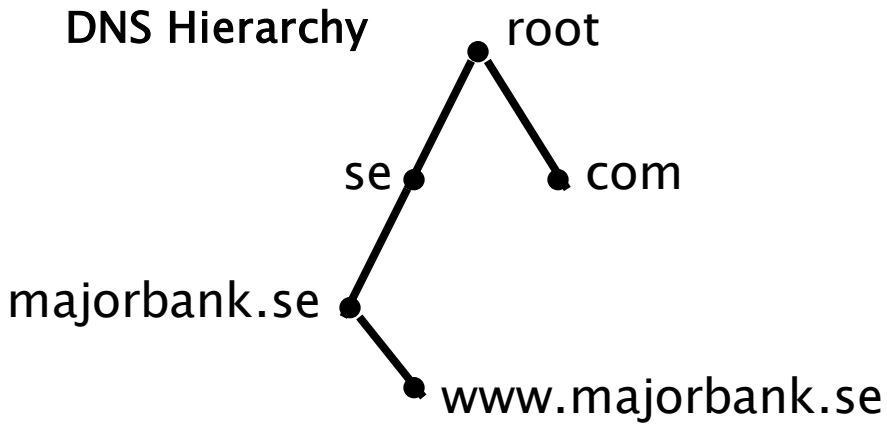
- CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
- DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents
- With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)

The Bad: DNSChanger - 'Biggest Cybercriminal Takedown in History' – 4M machines, 100 countries, $14M

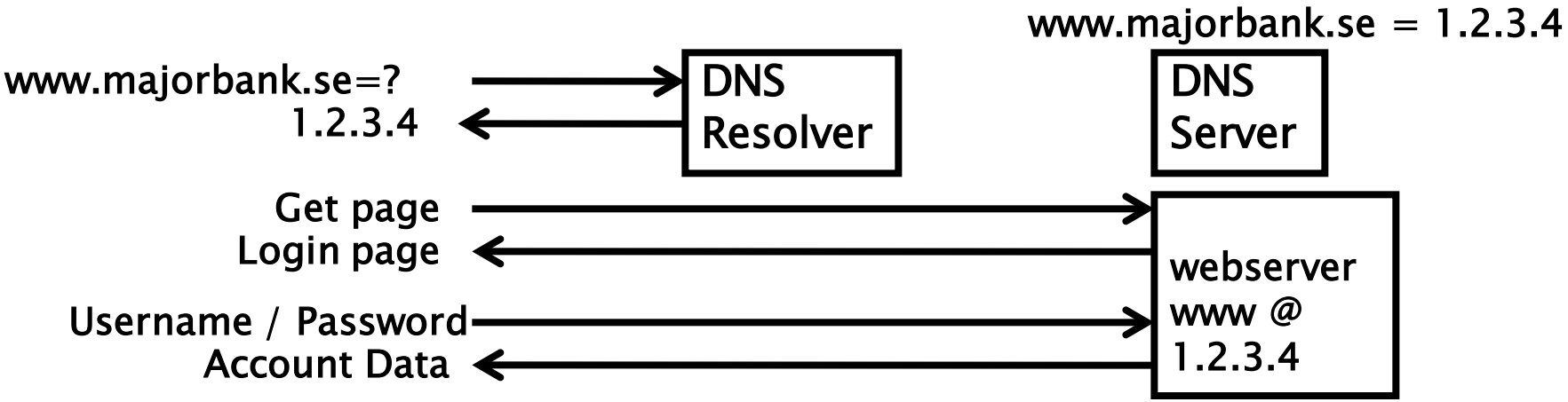
Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
End-2-end DNSSEC validation would have avoided the problems

The Internet's Phone Book - Domain Name System (DNS)

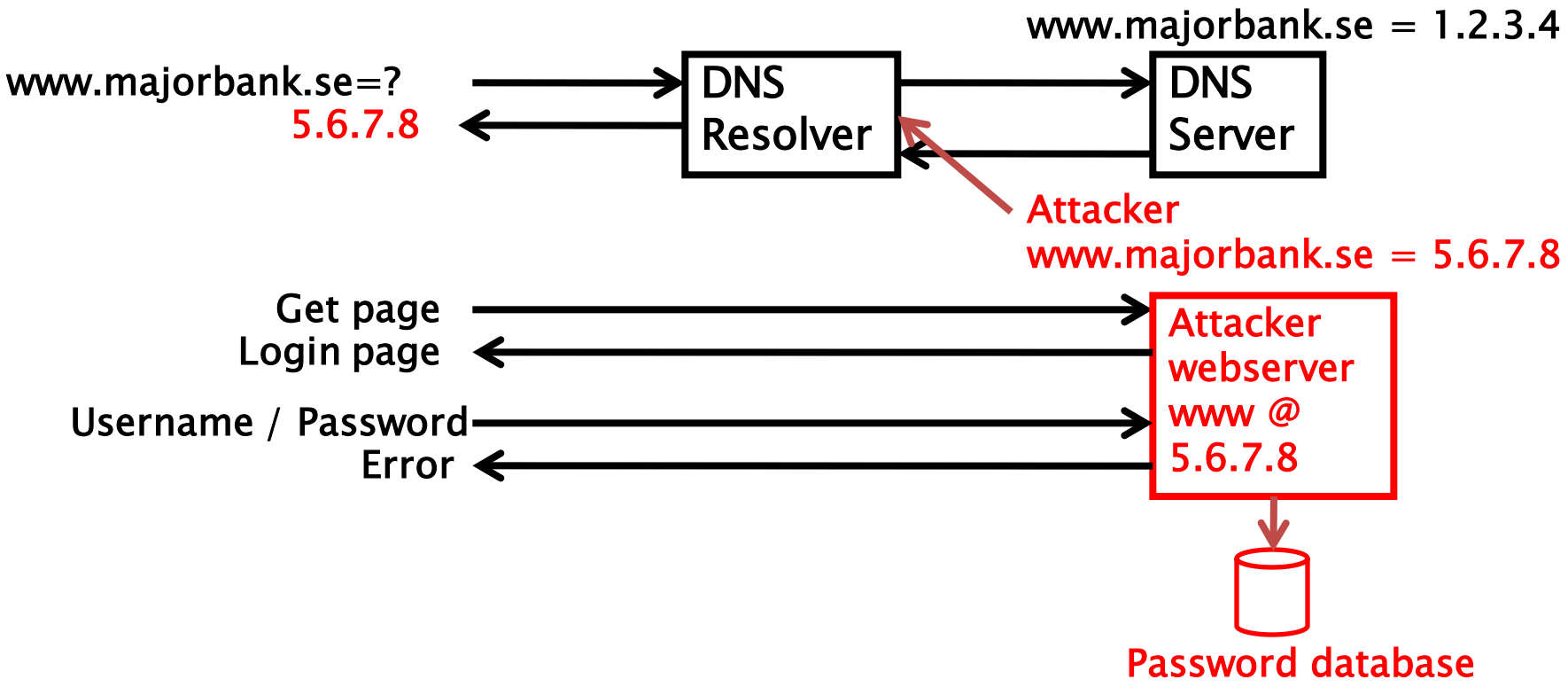




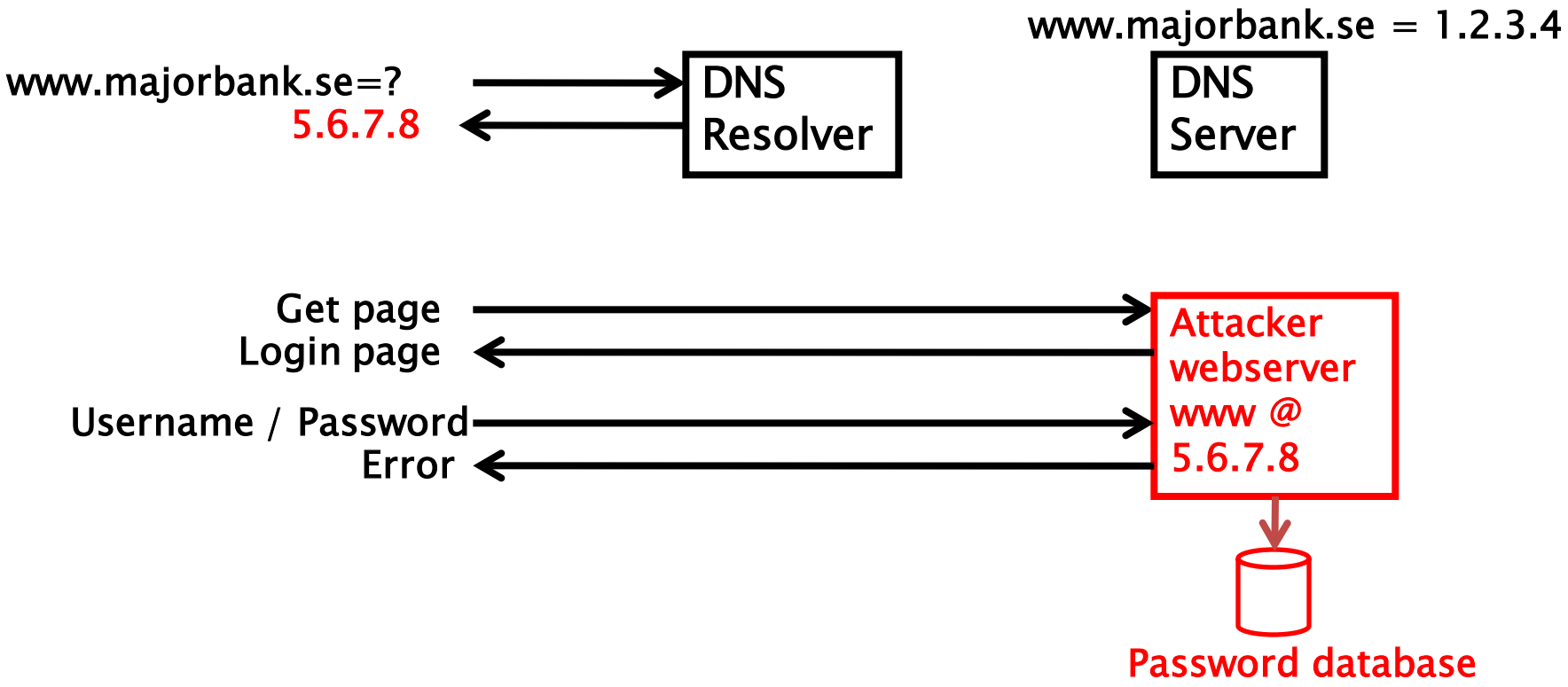
Caching Responses for Efficiency



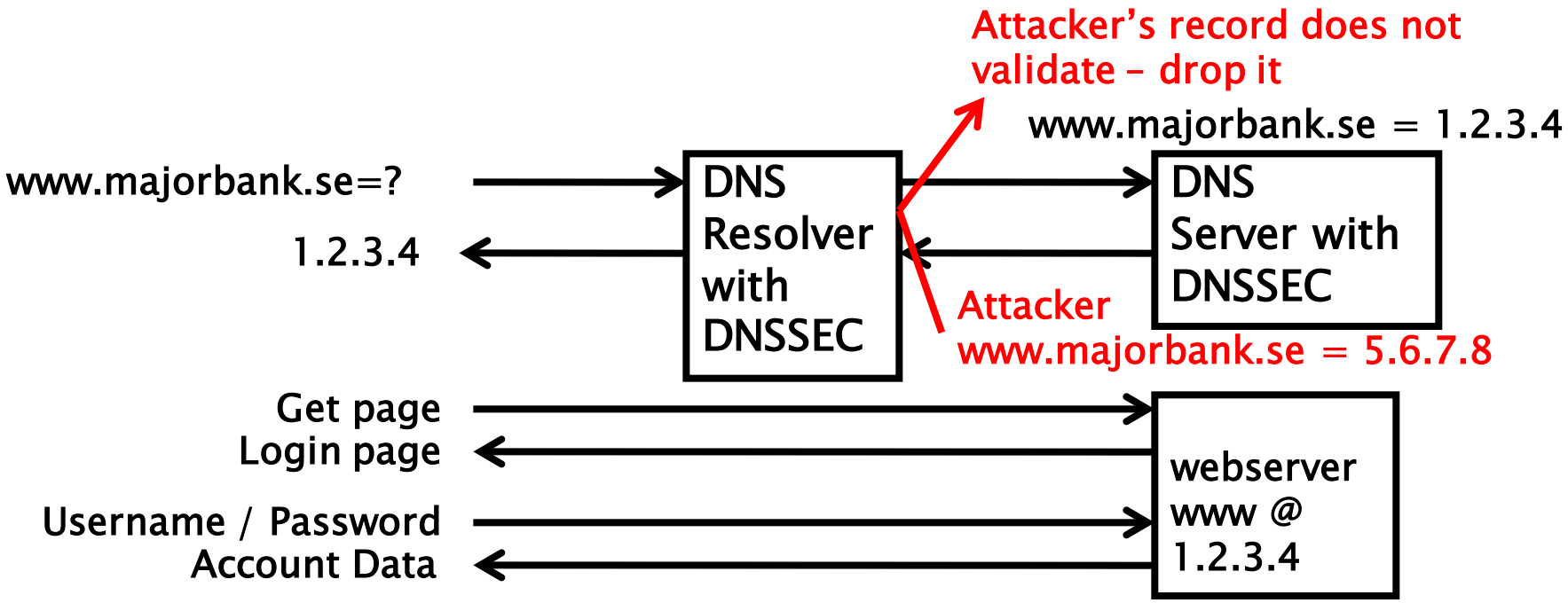
The Problem:
DNS Cache Poisoning Attack



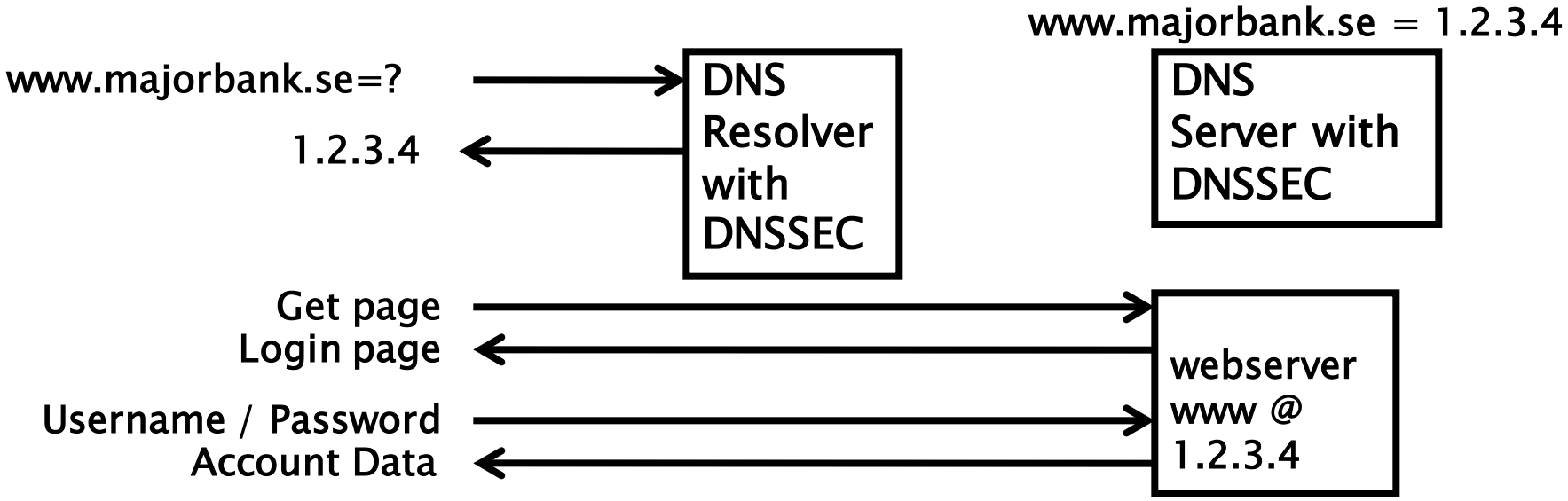
Argghh! Now all ISP customers get sent to attacker.



Securing The Phone Book - DNS Security Extensions (DNSSEC)

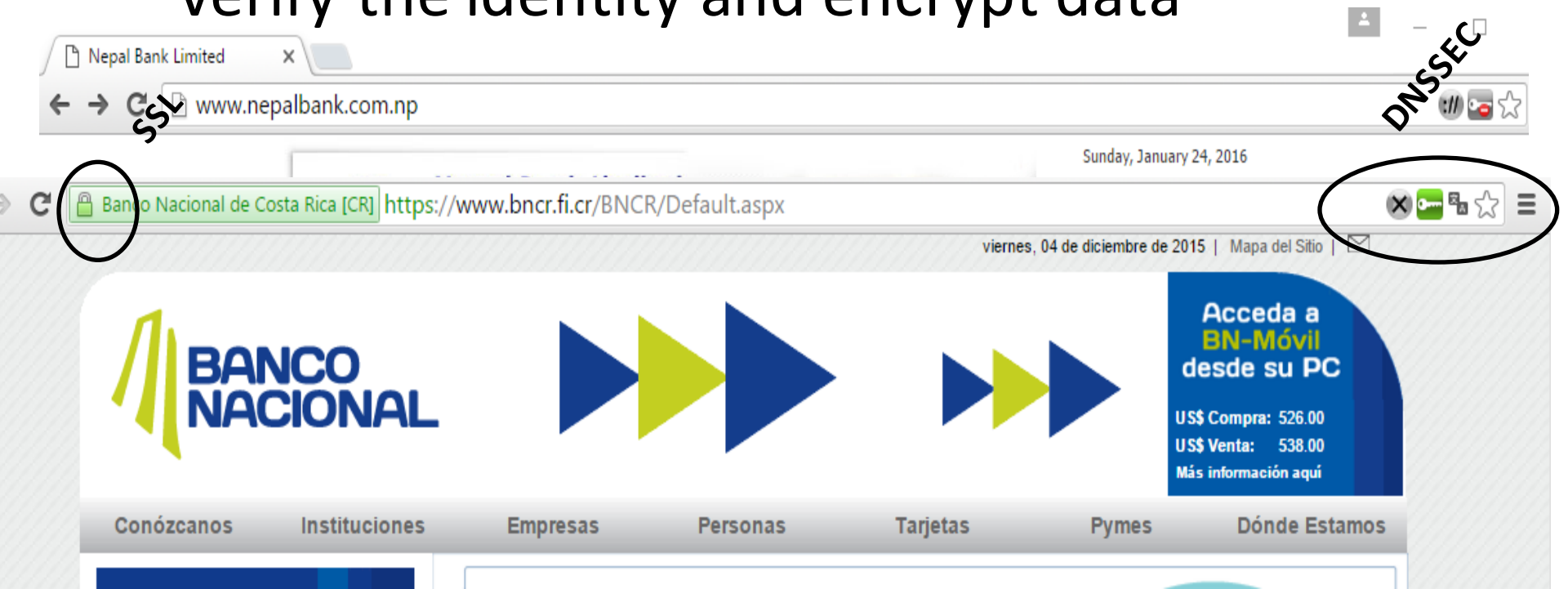


Resolver only caches validated records



Securing it

- DNS converts names (www.bncr.fi.cr) to numbers (201.220.29.26)
- Make sure we get the right numbers (DNSSEC)
- Verify the identity and encrypt data



The Bad: Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – "Iranian cyber army"
- 13 Aug 2010 - Chinese gmail phishing attack
- 25 Dec 2010 Tunisia DNS Hijack
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- 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

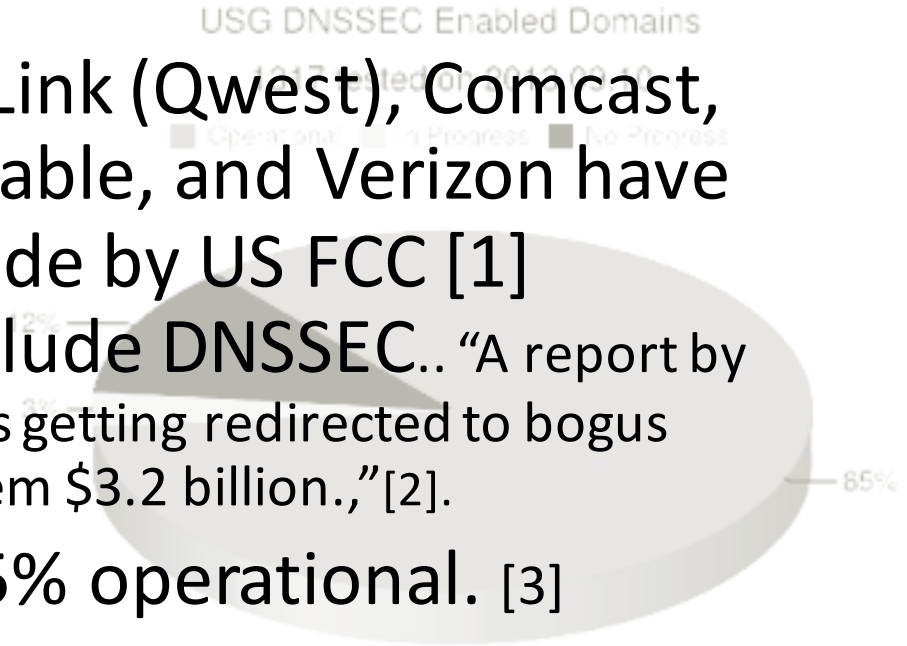
*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

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.

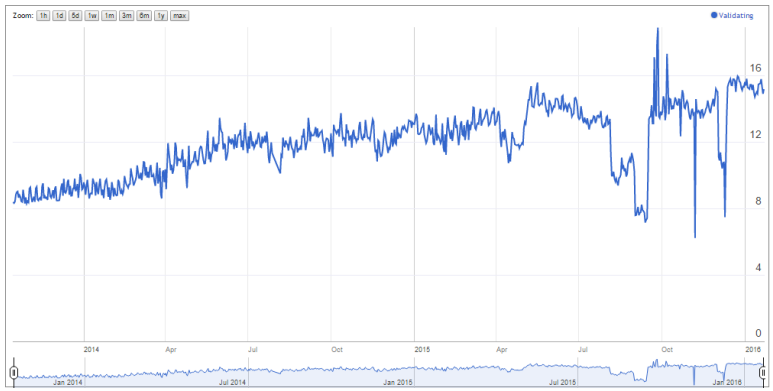
DNSSEC interest from governments

- Sweden, Brazil, Netherlands, Czech Republic and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,"[2].
- 2008 US .gov mandate. 85% operational. [3]

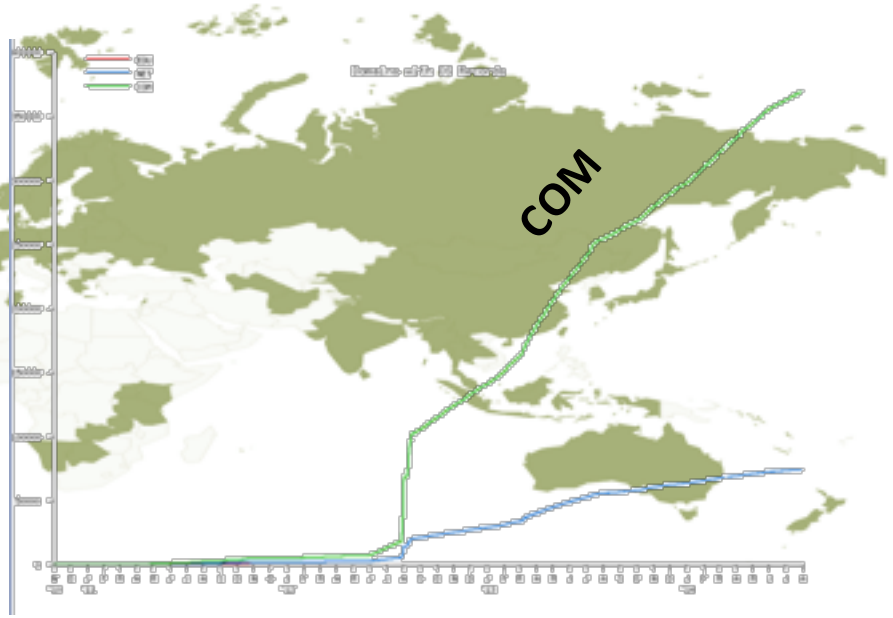


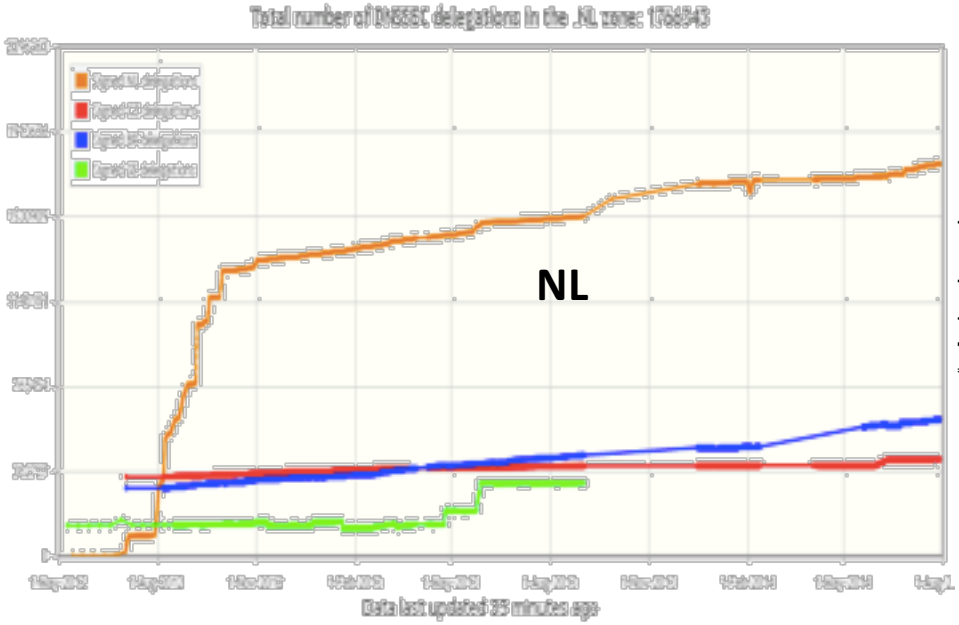
[1] FCC=Federal Communications Commission=US communications Ministry
[2] http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf
http://fedv6-deployment.antd.nist.gov/snap-all.html

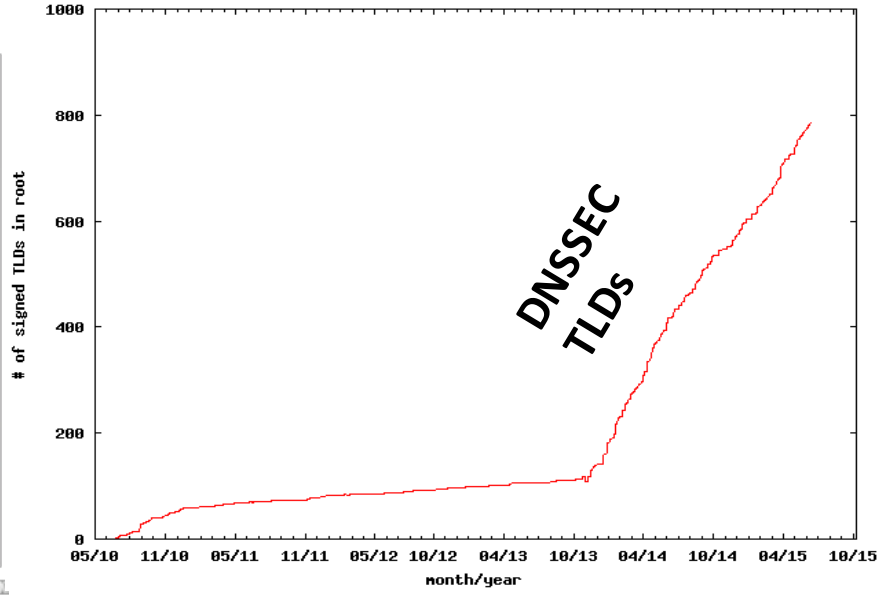
Use of DNSSEC Validation for World (XA)



Thank you Geoff Huston







DNSSEC - Where we are

- Deployed on 1034/1205 TLDs (23 Jan 2016 .az .in .af .tm .kg .cn .th .id .lk .se .de .ru .pф .com .uk .nl .fr .in .jp .us .my ايسيلم .asia .tw 台灣, .kr 한국 .net, .org, .post, +ntlds, .ibm .berlin)
- Root signed** and audited
- > 85% of domain names could have DNSSEC
- Required in new gTLDs. Basic support by ICANN registrars
- Growing ISP support* - ~16% end users "validate".
- 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 TLS certificates (RFC6698) and others
- Growing support from major players…(Apple iPhone/iPad, Google 8.8.8.8, hosting co Cloudflare DNSSEC by default, German email providers…)

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

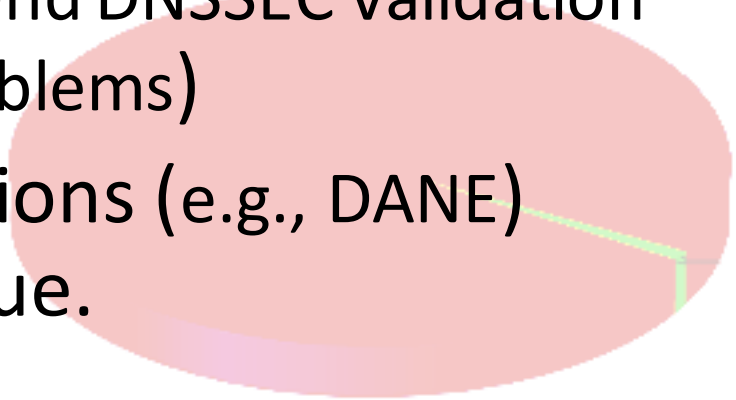
* COMCAST /w 20M and others; most ISPs in SE ,CZ.

**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…

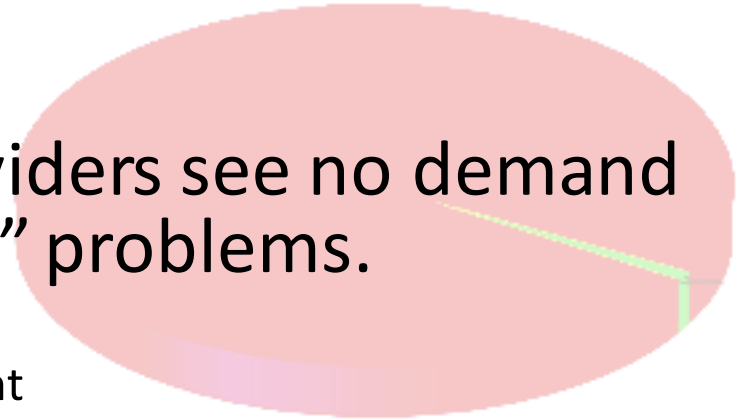
- But deployed on only ~2% of 2nd level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*, comcast.com).
- DNSChanger and other attacks highlight today's need. (e.g end-2-end DNSSEC validation would have avoided the problems)
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.



*** http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com**
http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html
http://www.nacion.com/2012-03-15/Tecnologia/Sitios-web-de-bancos-ticos-podran-ser-mas-seguros.aspx

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 and CDN support.
- Registrars*/CDNs/DNS providers see no demand leading to "chicken-and-egg" problems.



*but required by new ICANN registrar agreement

Who Can Implement DNSSEC

- Enterprises – Sign their zones and validate lookups
- TLD Operators – Sign the TLD
- Domain Name holders – Sign their zones
- Internet Service Providers – validate DNS lookups
- Hosting Provider – offer signing services to customers
- Registrars – accept DNSSEC records (e.g., DS)

ICANN

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 ICANN, ISOC and other organizations offering DNSSEC education and training

DNSSEC: A Global Platform for Innovation

or..

I* $mell opportunity !

Game changing Internet Core Infrastructure Upgrade

- “More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. ..” – Vint Cerf (June 2010)

For Techies and other Dreamers

Too many CAs. Which one can we trust? DNSSEC to the rescue….

CA Certificate roots ~1482
Symantec, Thawte, Godaddy

DNSSEC root - 1

Internet of Things
IoT

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
"Free SSL"
certificates for Web
and e-mail and "trust
agility" **DANE**

Cross-
organizational and
trans-national
authentication and
security

DANE and other yet to be
discovered security
innovations, enhancements,
and synergies

Crypto currencies
and e-commerce?

E-mail security SMIME,
DKIM RFC4871

Securing VoIP

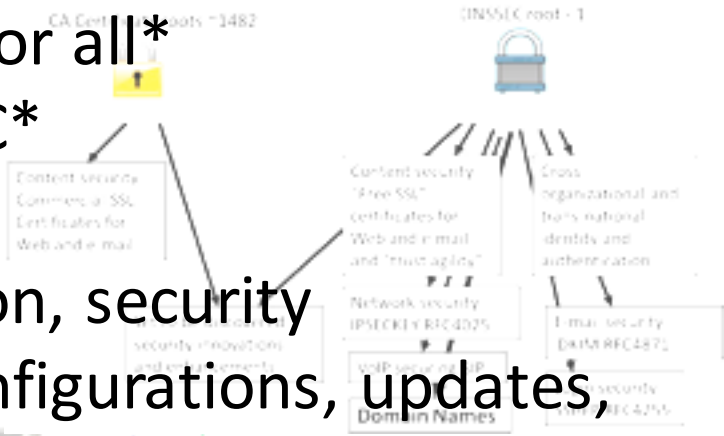
Login security
SSHFP RFC4255

Domain Names

https://www.eff.org/observatory
http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

Opportunity: New Security Solutions

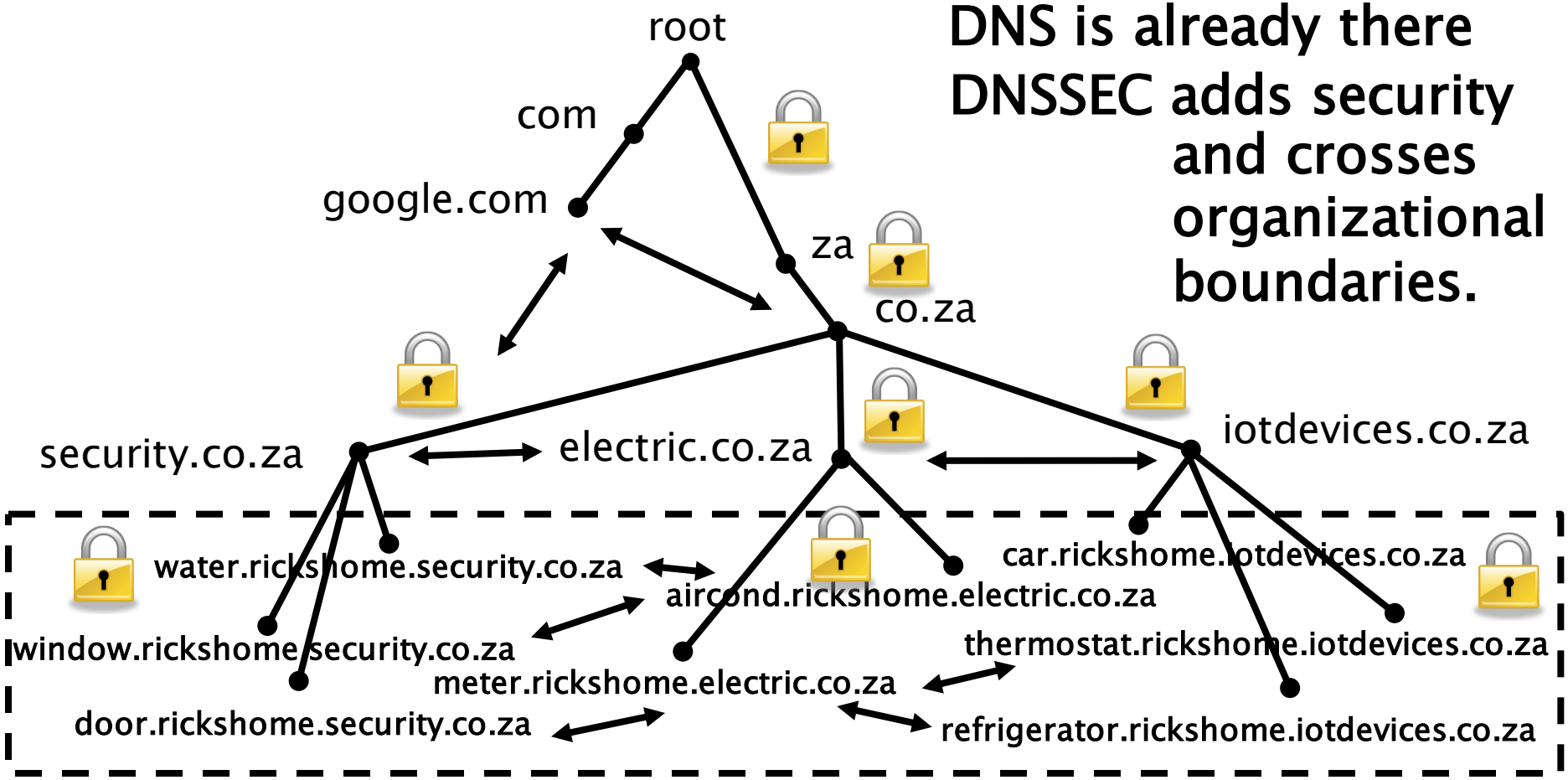
- Improved Web SSL and certificates for all*
- Secured e-mail (SMTP+S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational authentication, security
- Secured content delivery (e.g. configurations, updates, keys) – Internet of Things
- Securing Smart Grid efforts
- Increasing trust in e-commerce
- Securing cryptocurrencies and other new models
- First global FREE PKI



A good ref http://www.internetsociety.org/deploy360/dnssec/

***IETF standards complete and more currently being developed**

A thought: Scalable Security for IoT



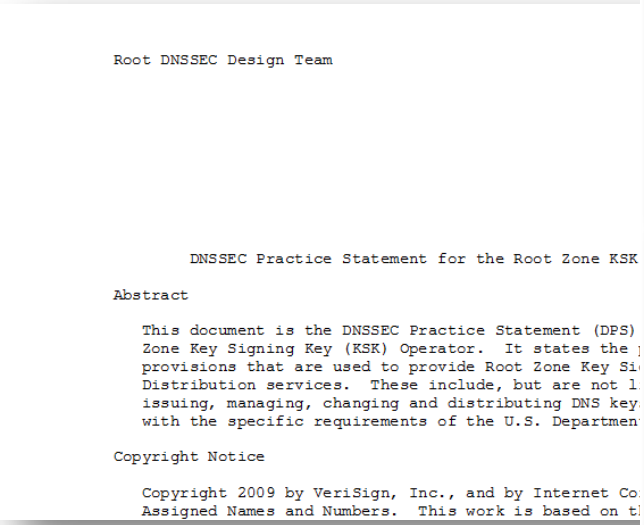
Animated slide

DNSSEC: Internet infrastructure upgrade to help address today's needs and create tomorrow's opportunity.

More Techie stuff..
Hmm…how do I trust it?
(transparency transparency transparency!)

ICANN DNSSEC Deployment @Root

- **Multi-stakeholder, bottom-up trust model* /w 21 crypto officers from around the world**
- **Broadcast Key Ceremonies and public docs**
- **SysTrust audited**
- **FIPS 140-2 level 4 HSMs**



Root DNSSEC Design Team

DNSSEC Practice Statement for the Root Zone KSK

Abstract

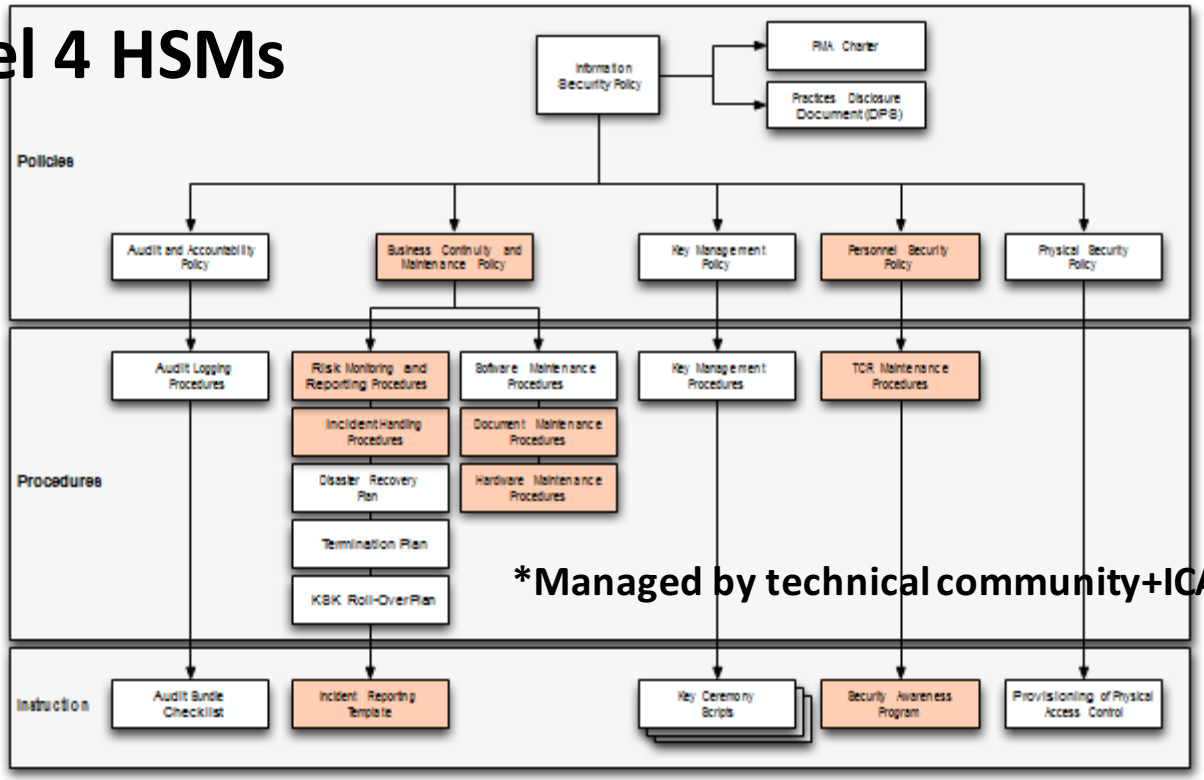
This document is the DNSSEC Practice Statement (DPS) Zone Key Signing Key (KSK) Operator. It states the provisions that are used to provide Root Zone Key Si Distribution services. These include, but are not l issuing, managing, changing and distributing DNS key with the specific requirements of the U.S. Departmen

Copyright Notice

Copyright 2009 by VeriSign, Inc., and by Internet Co Assigned Names and Numbers. This work is based on t

Root DPS

DNSSEC Practice Statement



*Managed by technical community+ICANN

ICANN DNSSEC Deployment @Root (and elsewhere)

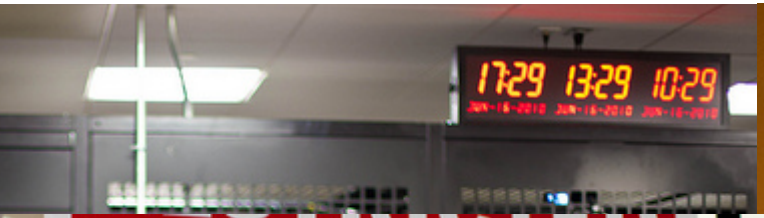
FIPS 140-2 level 4

SysTrust

Next .. ISO 19790

DCID 6/9
"SCIF" spec

http://www.flickr.com/photos/kjd/sets/72157624302045698/



N Sepulveda Blvd
E Maple Ave
Indiana Ct
1920 E Maple Ave, El Segundo, CA 90

January 27, 2010

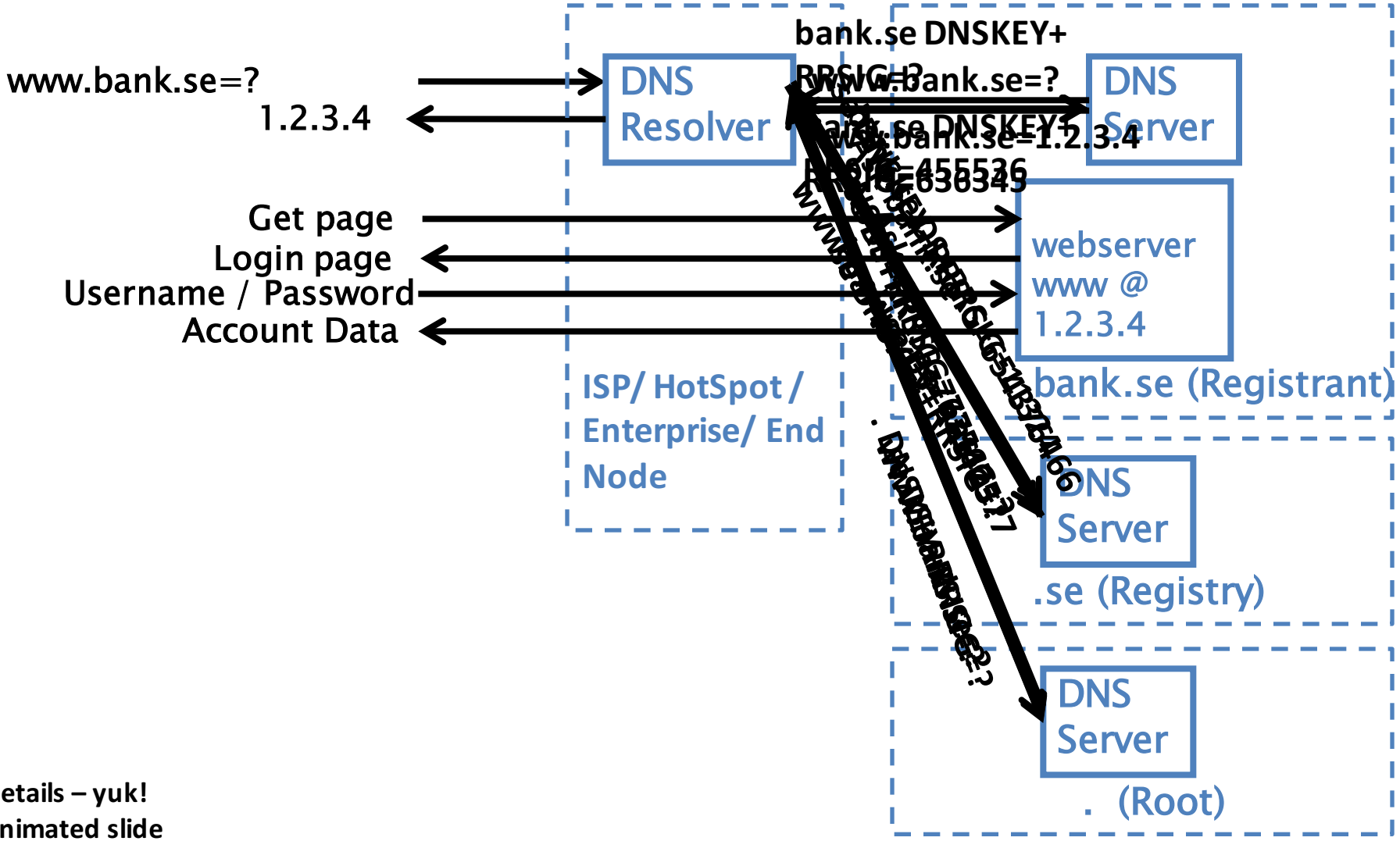
ICA

Photos: Kim Davies

DNSSEC: Internet infrastructure upgrade to help address today's needs and create tomorrow's opportunity.

Tech Details of a DNSSEC Lookup

The Internet's Phone Book - Domain Name System (DNS+DNSSEC)



Details – yuk!
Animated slide