The Business Case for DNSSEC

Medellin, Colombia 2013

5 May 2013

richard.lamb@icann.org

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.

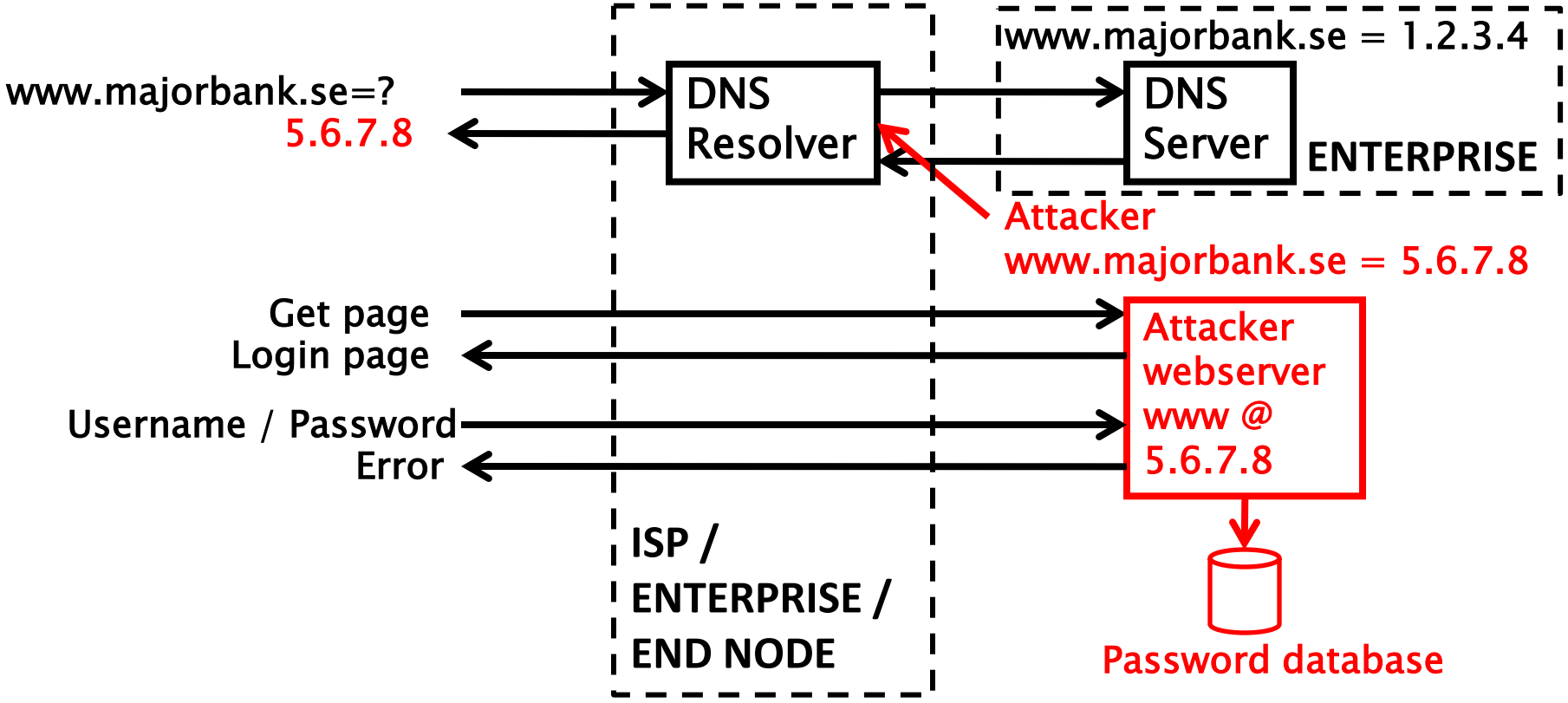
Where DNSSEC fits in

- DNS converts names (www.uob.com.sg) to numbers (203.116.108.5)
- ..to identify services such as www and e-mail
- ..that identify and link customers to business and visa versa

Where DNSSEC fits in

- ..but 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)

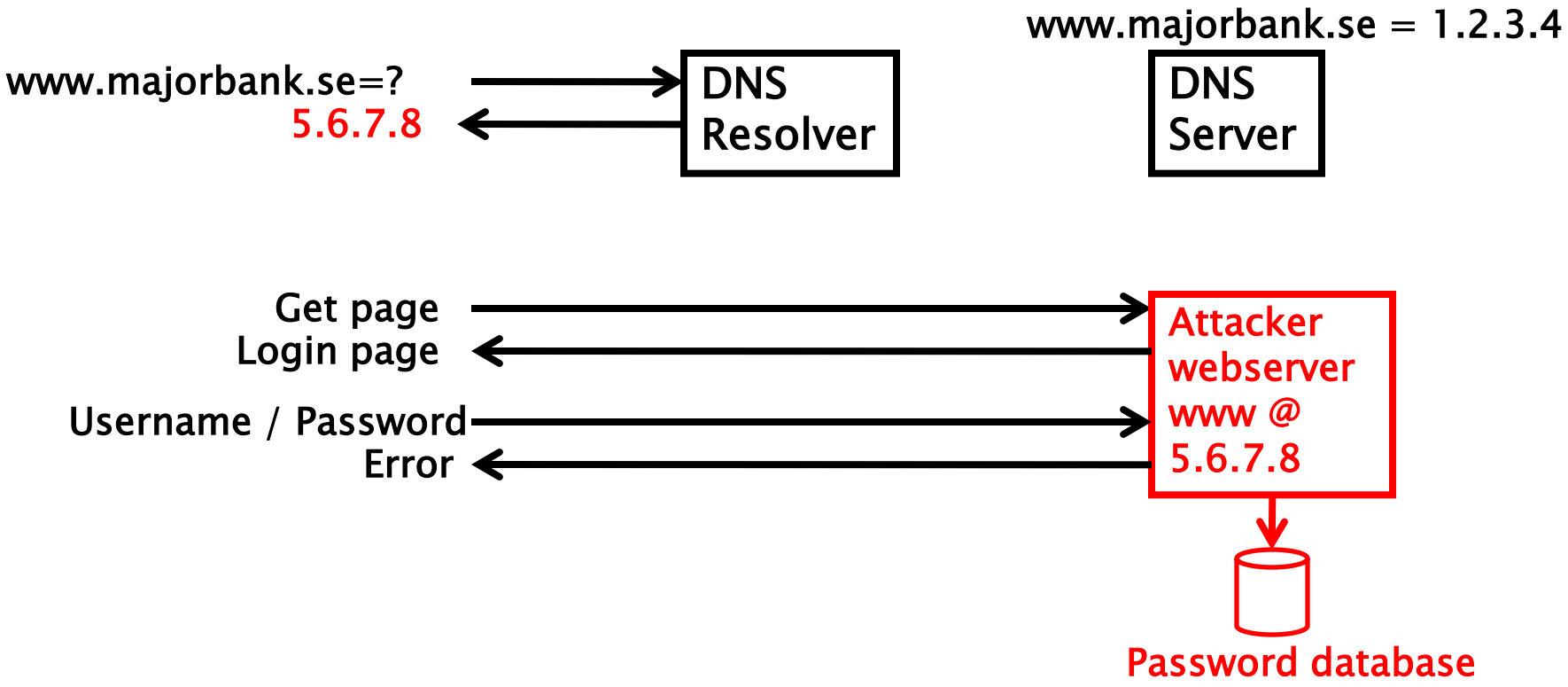
The Original Problem: DNS Cache Poisoning Attack



Animated slide

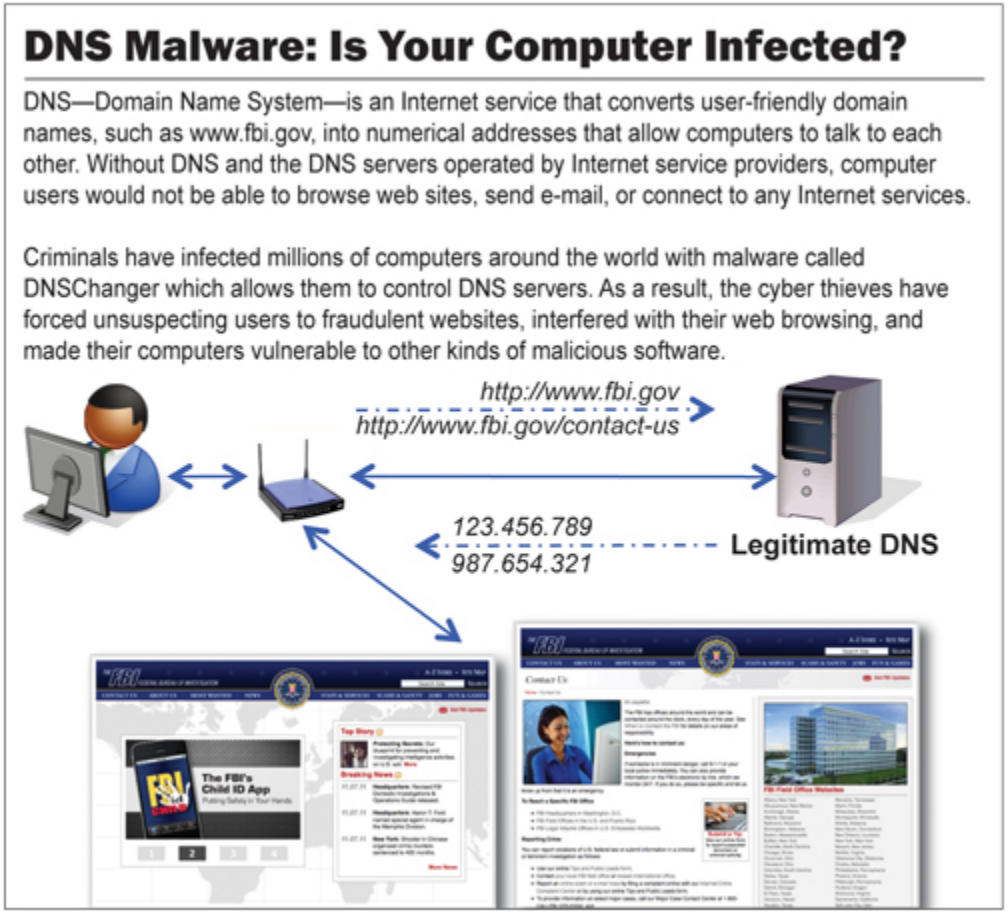
detailed description at: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Argghh! Now all ISP customers get sent to attacker.



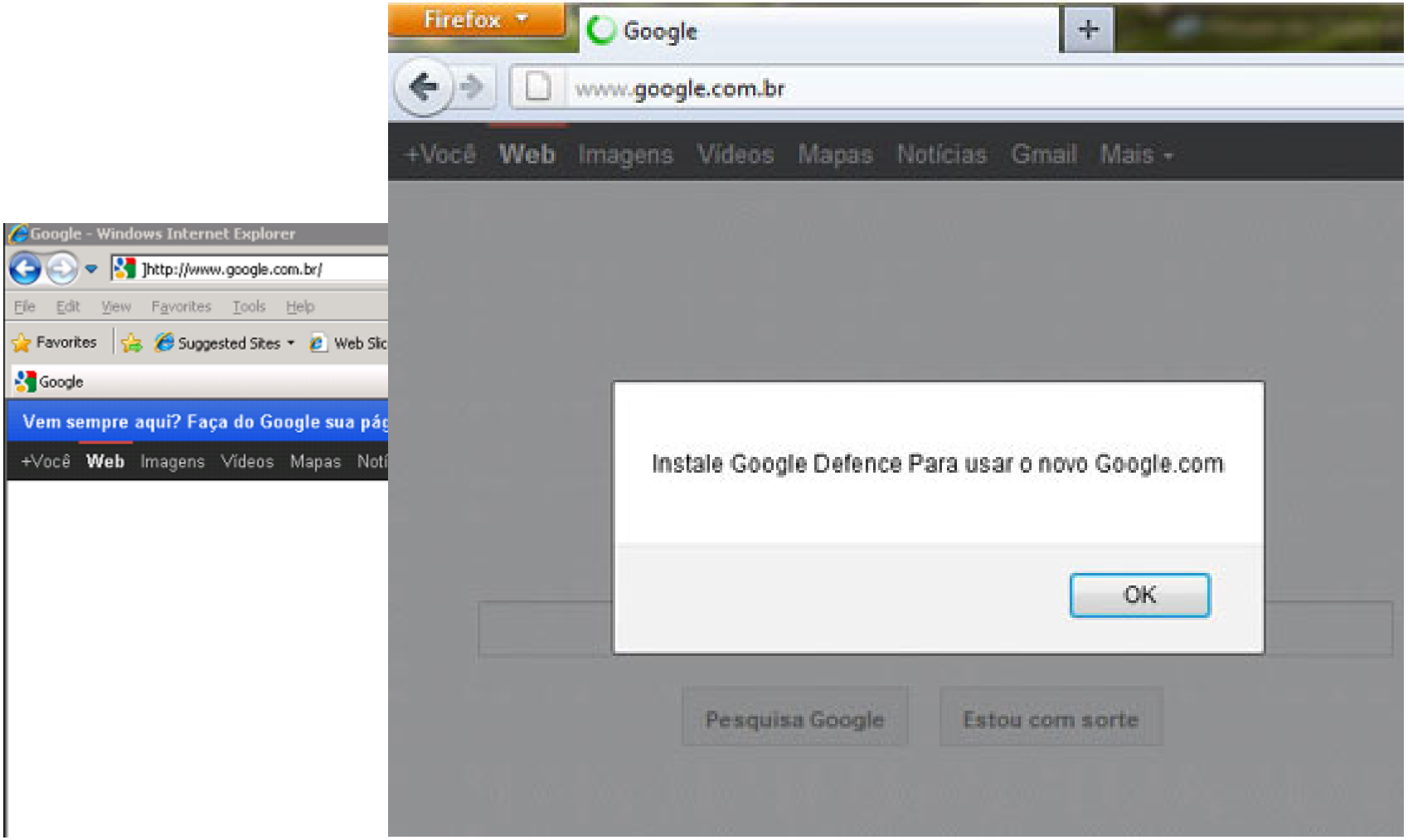
Animated slide

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 Bad: Brazilian ISP fall victim to a series of DNS attacks



7 Nov 2011 http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

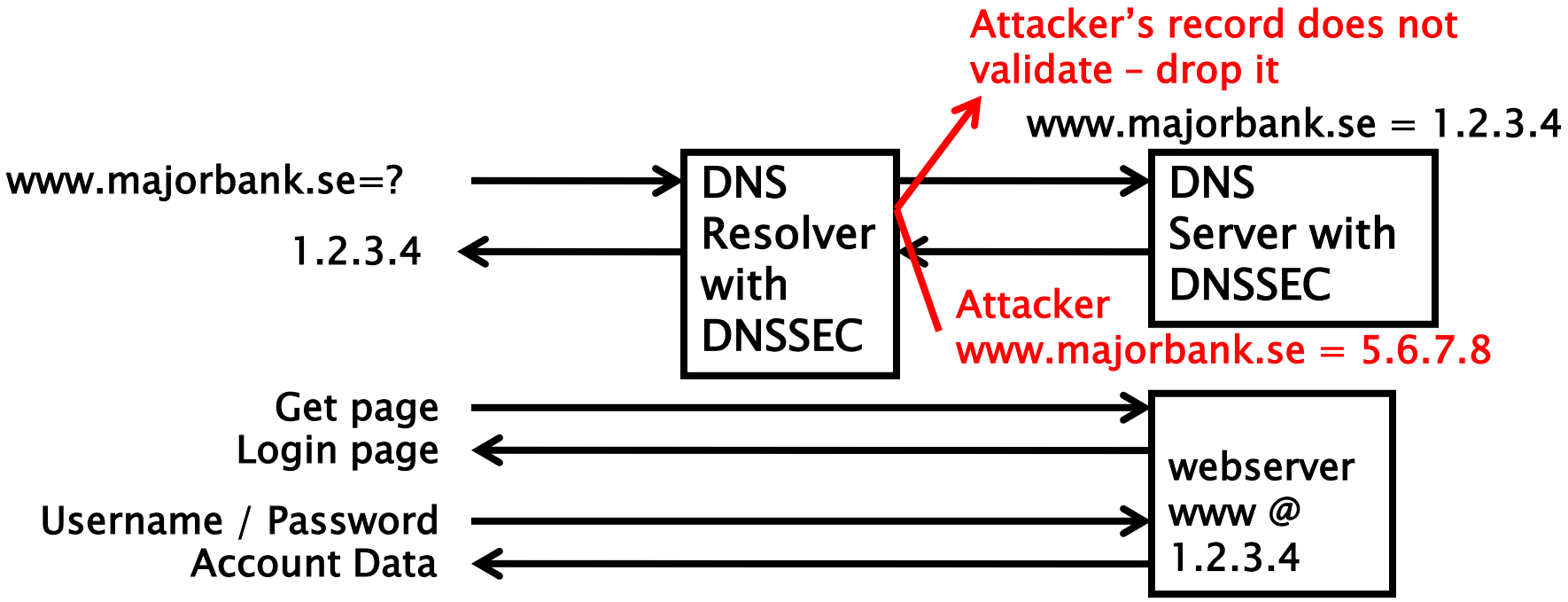
End-2-end DNSSEC validation would have avoided the problems

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.

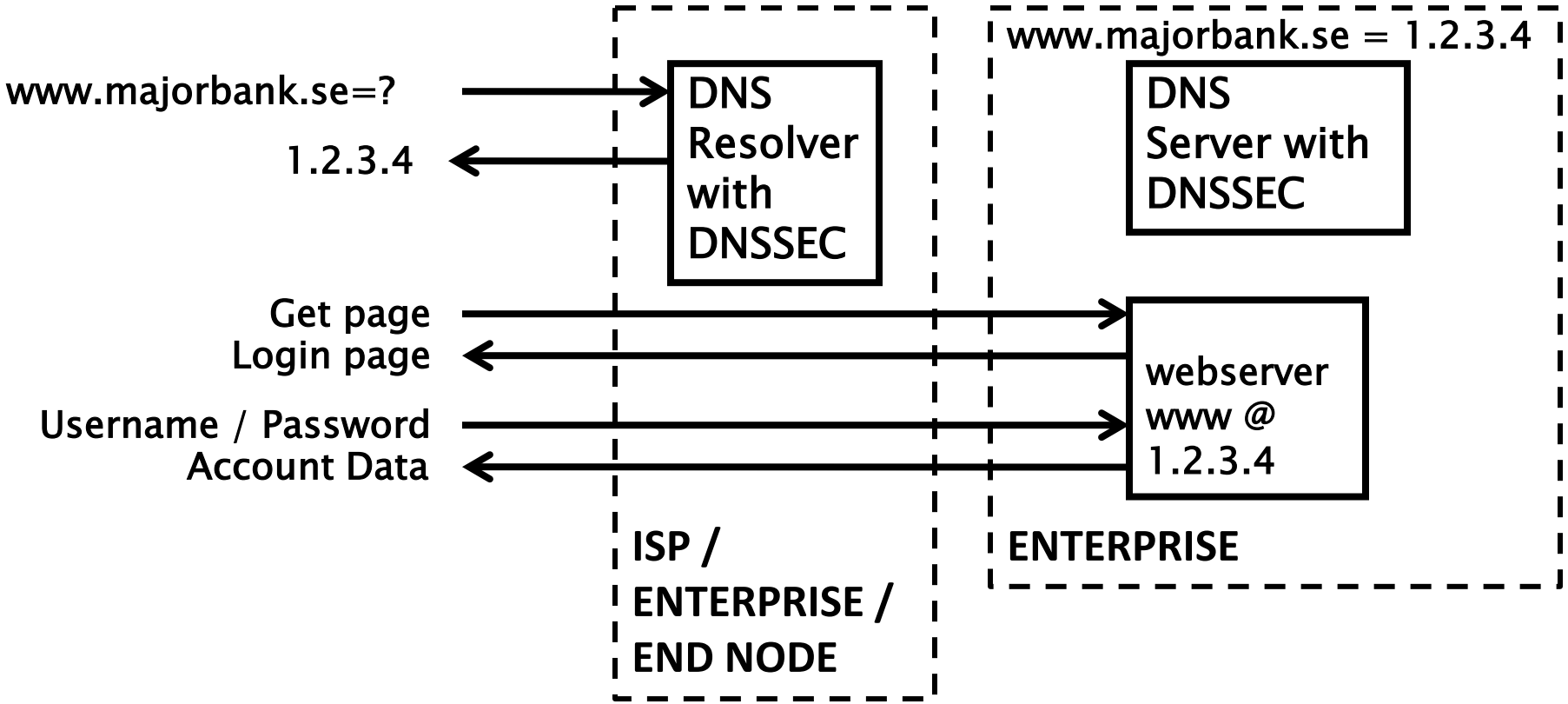
*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

The Good: Securing DNS with DNSSEC



Animated slide

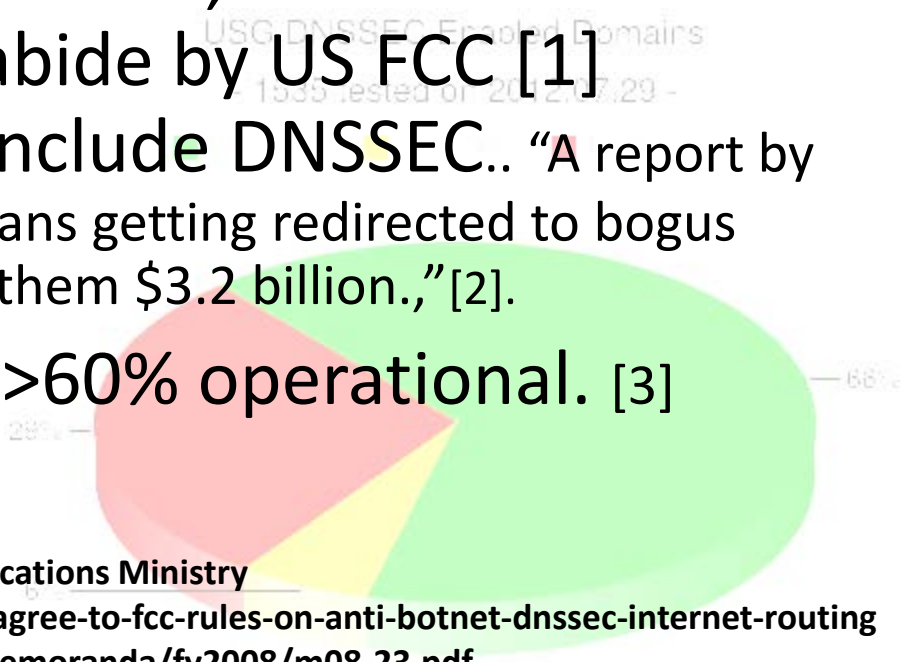
The Good: Resolver only caches validated records



Animated slide

DNSSEC interest from governments

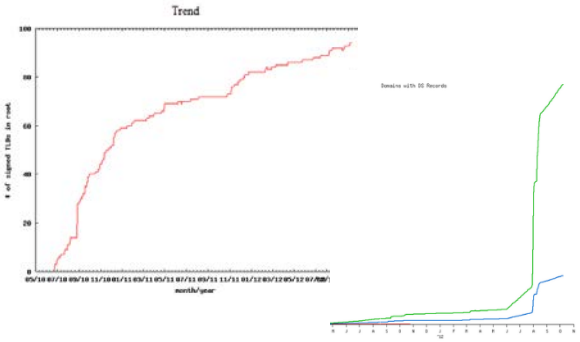
- Sweden, Brazil, Netherlands and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,"[2].
- 2008 US .gov mandate. >60% operational. [3]

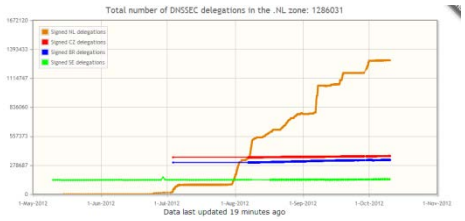


[1] FCC=Federal Communications Commission=US communications Ministry
[2] http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

Security as Differentiator and Edge

- Differentiator
  - Increased cyber security awareness for govts and industry
  - Major ISP says security now on checklist for customers
- DNSSEC Service and Support
  - 102/317 TLDs (e.g., .jp, .kr, .ru, .com,
  - Growing ISPs adoption*
  - Available to 86% of domains
  - Vendor support (ISC/BIND, Microsoft..)
  - gTLDs (e.g., .bank, .search) require it





***COMCAST Internet (18M), TeliaSonera SE, Sprint,Vodafone CZ,Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..**

DNSSEC - Where we are

- Deployed on 105/317 TLDs (.my .th .mm .in .kg .lk .nc .nz .la .pw .tv .kr .jp .ru .pф .de .my ملیسیا .asia .tw 台灣, .kr 한국 .com .net, .post, … and soon .cn)
- Root signed** and audited
- >86% of domain names could have DNSSEC
- Required in new gTLDs
- Growing ISP support*
- 3rd party signing solutions: GoDaddy, Binero, VeriSign…***
- Growing S/W H/W support: NLNetLabs/NSD+Unbound, ISC/BIND, Microsoft, PowerDNS, Secure64…?openssl, mozilla DANE support?
- IETF standard on DNSSEC SSL certificates (RFC6698)
- Growing support from major players…(IOS, 8.8.8.8,…)

***COMCAST Internet (18M), TeliaSonera SE, Sprint,Vodafone CZ,Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..**

****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**

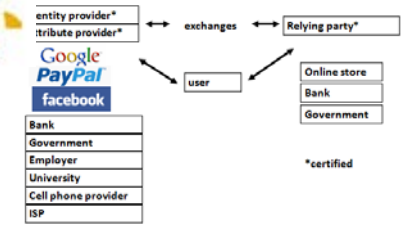
+1-202-709-5262
VoIP

US-NSTIC effort

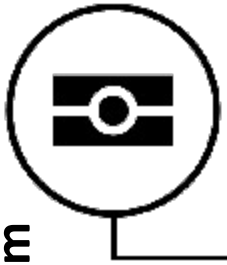
DNS is a part of all IT ecosystems

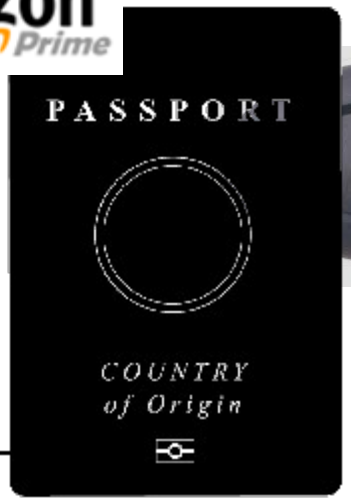
Google
OpenID
facebook
eBay
AADHAAR
PayPal
amazon Prime

OECS ID effort



e-Passport symbol



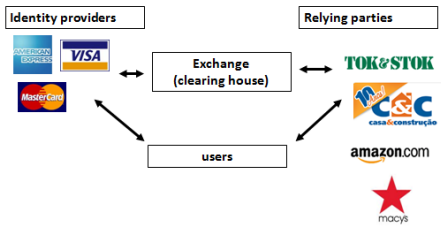


ICP Brasil
O Brasil na era da certificação digital

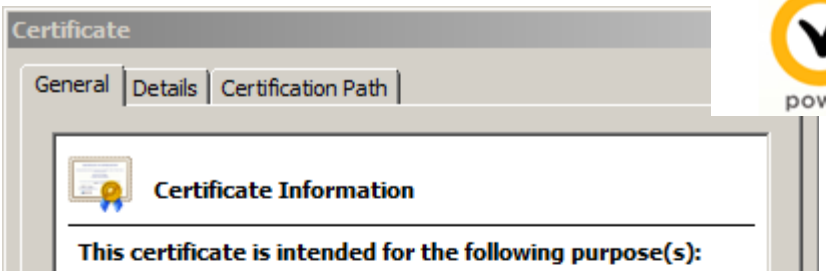
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online®

Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign

lamb@xtcn.com

mydomainname.com

The Bad: SSL Dilution of Trust
The Good: DNSSEC = Global "free" PKI

CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

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

Cross-
organizational and
trans-national
identity and
authentication

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

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

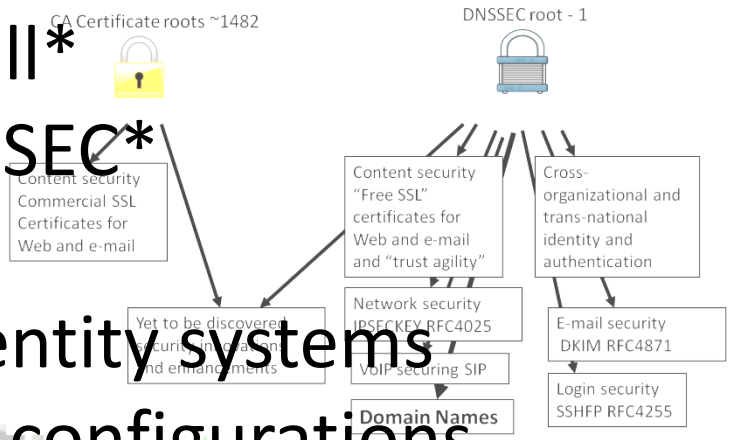
E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

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

Opportunity: New Security Products

- Improved Web SSL and certificates for all*
- Secured e-mail (S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational digital identity systems
- Secured content delivery (e.g. configurations, updates, keys)
- Securing Smart Grid efforts
- A global PKI
- Increasing trust in e-commerce

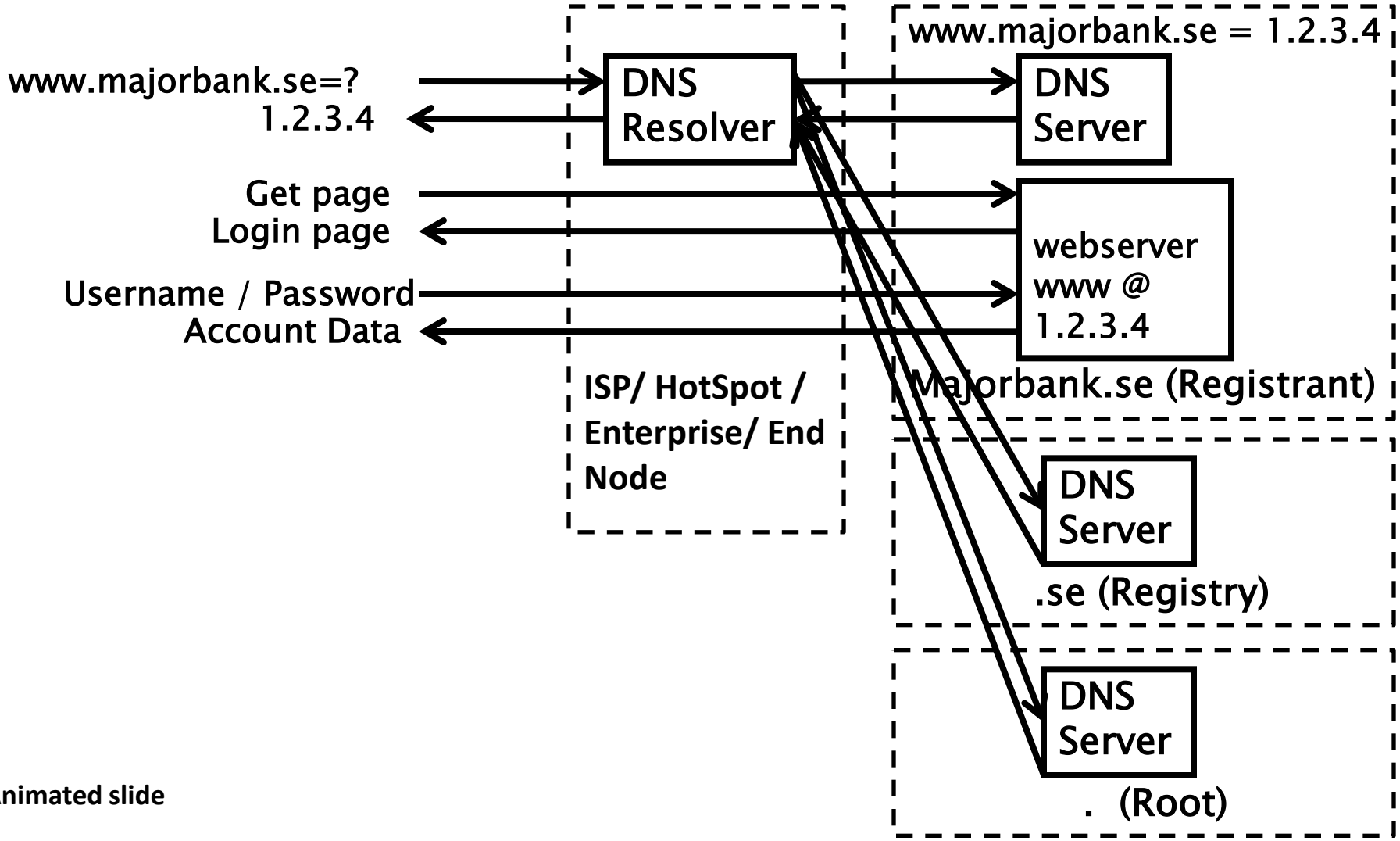


A good ref http://www.internetsociety.org/deploy360/dnssec/

***IETF standards complete or currently being developed**

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

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



Animated slide