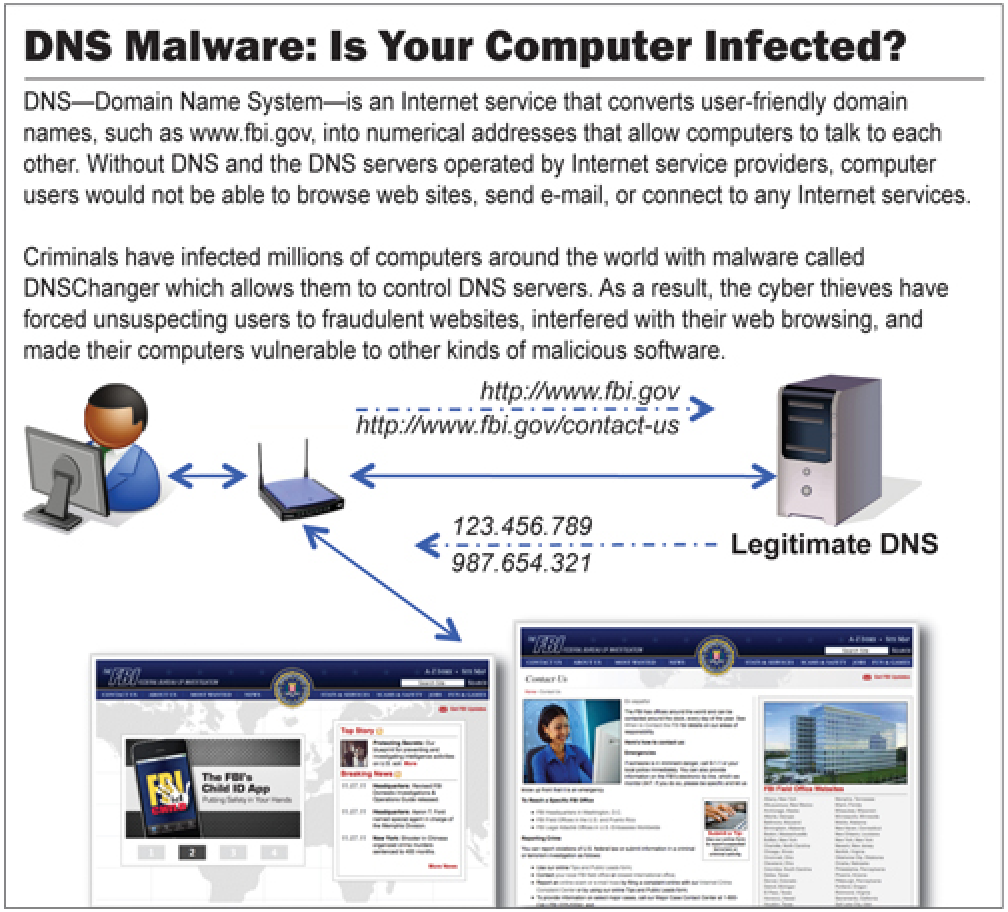
DNSSEC: A Game Changer

ICCS 2012
January 9, 2012
New York, NY
richard.lamb@icann.org

- The Internet did not have security designed into it.

- But has demonstrated time and again that it is a platform for innovation - good and bad.

The BAD: DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4 mil (1/2 mil in US)



DNS Malware: Is Your Computer Infected?

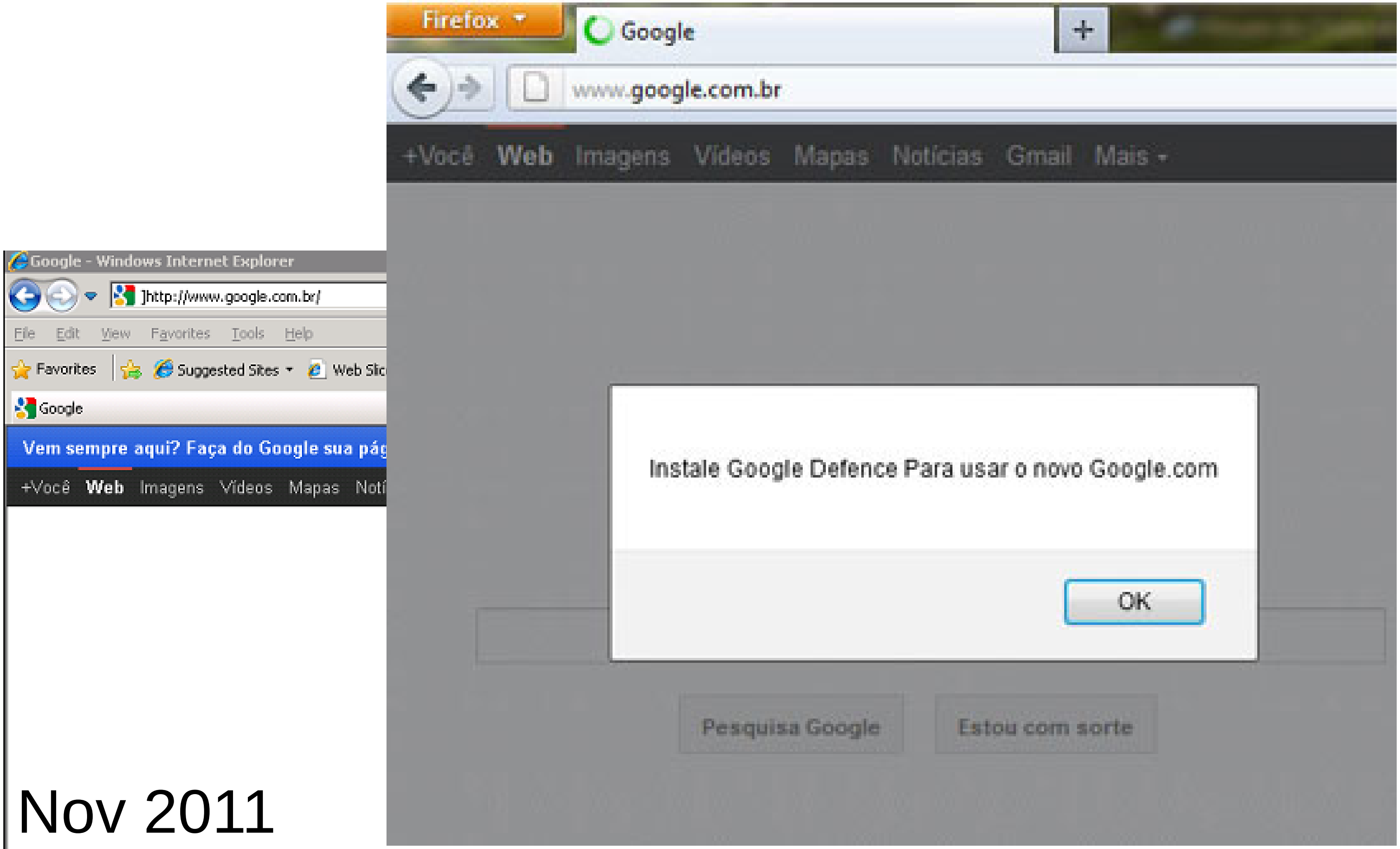
DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

9 Nov 2011

http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

The BAD: Brazilian ISP fall victim to a series of DNS attacks



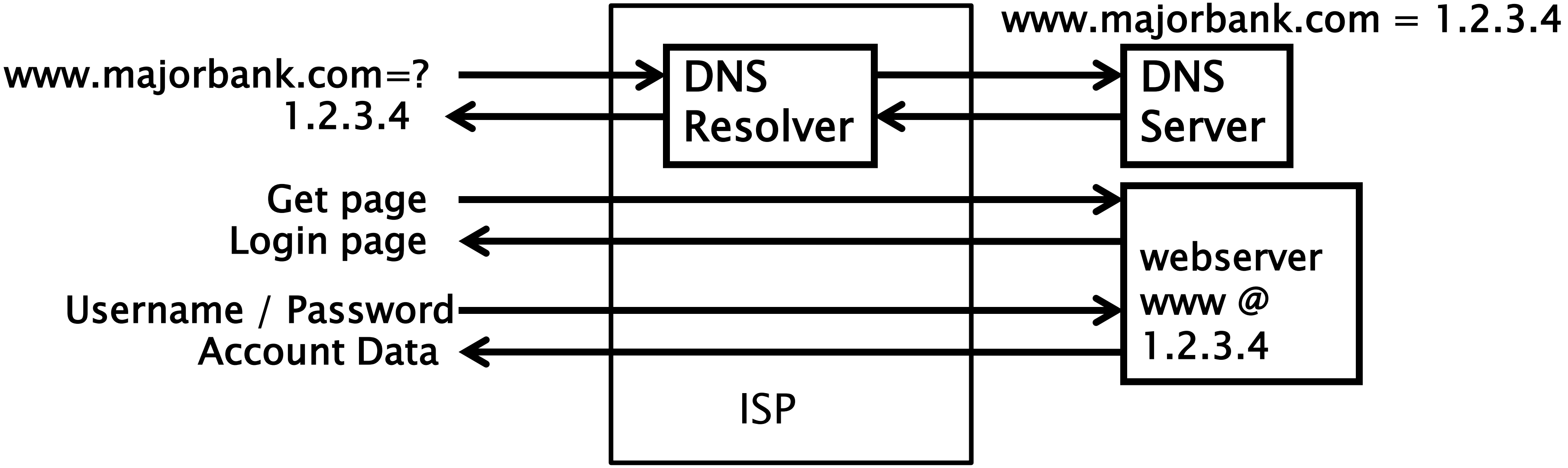
Instale Google Defence Para usar o novo Google.com

Firefox
Google
www.google.com.br
+Você Web Imagens Vídeos Mapas Notícias Gmail Mais
OK
Pesquisa Google
Estou com sorte
Google - Windows Internet Explorer
]http://www.google.com.br/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slic
Google
Vem sempre aqui? Faça do Google sua pág
+Você Web Imagens Vídeos Mapas Notí

7 Nov 2011

http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

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



www.majorbank.com = 1.2.3.4

www.majorbank.com=?

1.2.3.4

DNS Resolver

DNS Server

Get page

Login page

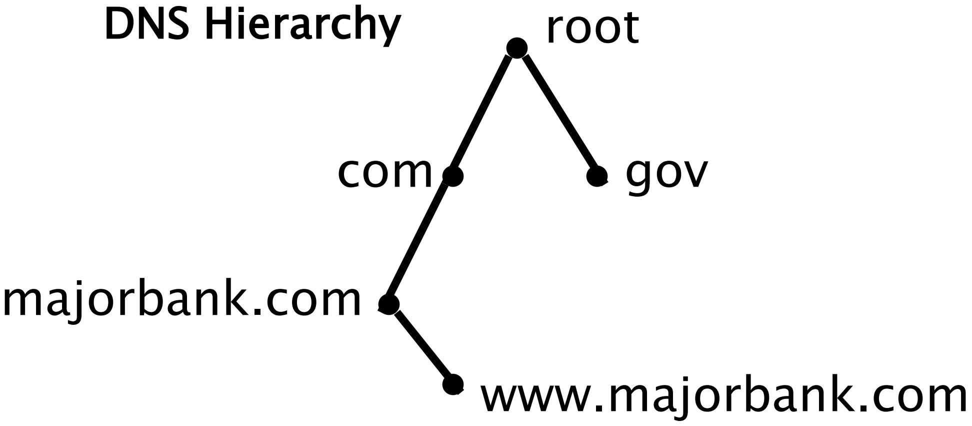
Username / Password

Account Data

webserver www @ 1.2.3.4

ISP

DNS Hierarchy



root

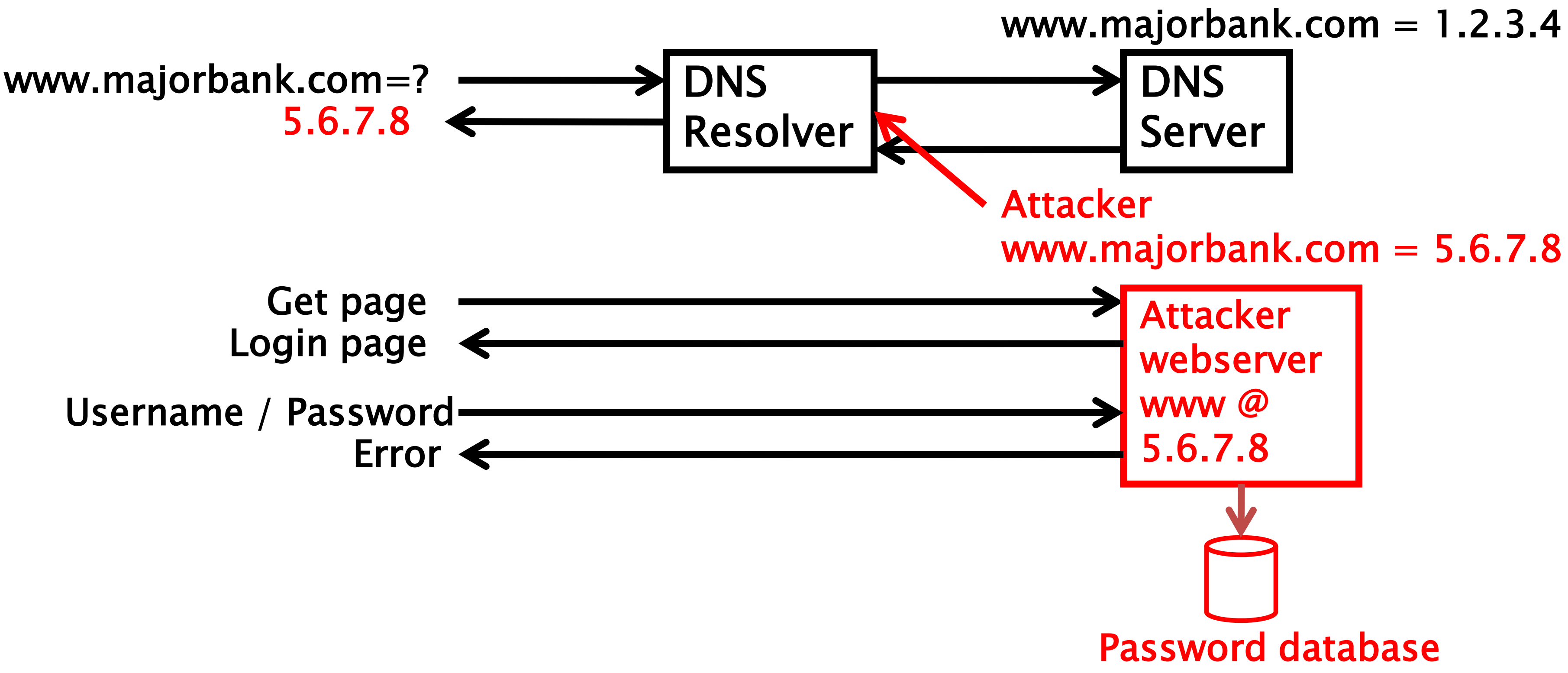
com

gov

majorbank.com

www.majorbank.com

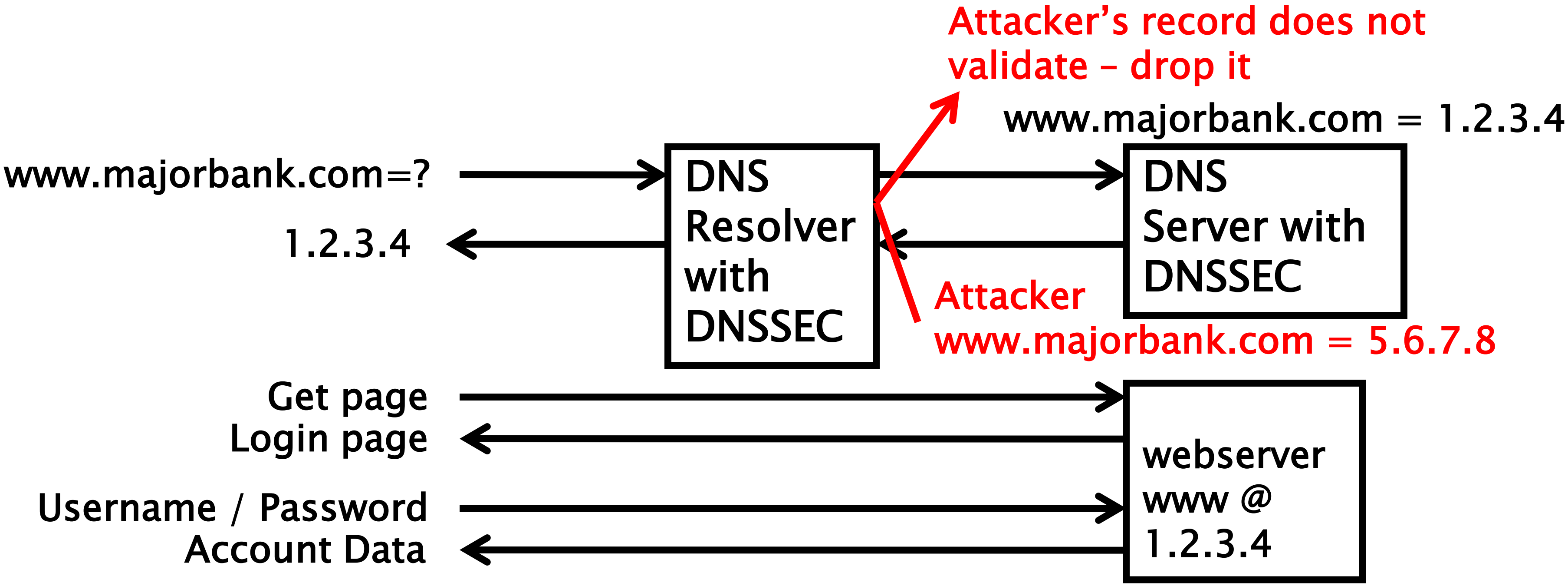
The BAD: DNS Cache Poisoning Attack



3 Aug 2008 Dan Kaminsky reveals shortcut

http://www.seattlepi.com/local/article/Seattle-security-expert-helped-uncover-major-1281123.php

Securing The Phone Book - DNS Security Extensions (DNSSEC)



The GOOD: DNSSEC

- Add keys to hierarchy and compute digital signatures. Keep it backward compatible
- Based on over 15 years of global technical community development (in IETF) after discovery of vulnerability

The GOOD: DNSSEC

- Listen to calls from global community for deployment:
  - Internet community (e.g., RIPE, APNIC, ccNSO…)
  - Governments (e.g., USG:DHS/OMB/NIST, EU members)
  - Business (e.g., Kaminsky 2008, Press)

Deploying it

- Problem
  - Bureaucracy and Fear: Hard to change anything that has not changed since 1983. Many excuses not to.
  - root - An internationally agreed to single key – right
  - Trust me - I will manage the root key. ..uh huh.

Look at other International efforts, e.g.,

- ICAO PKD
- Long top down development
- But not a single hierarchy
- Countries (27) pick-up / deposit certificates at ICAO contracted repository in Singapore

Approach

- Eliminate excuses and lead by example – start at root
- Solution
  - Multi-stakeholder – get buy in up front
  - Bottom up – like the Internet itself
  - Transparency and Choice
  - Draw from existing secure practices and trusted models
- Public-private partnership with US Department of Commerce and VeriSign (existing DNS management partner)

DNSSEC at the root: result

- Deployed 15 July 2010
- Completed in ~2years
- Biggest upgrade to the Internet’s core infrastructure in 20 years
- Set the stage for deployment in rest of hierarchy (e.g., top level domains, end user domains)

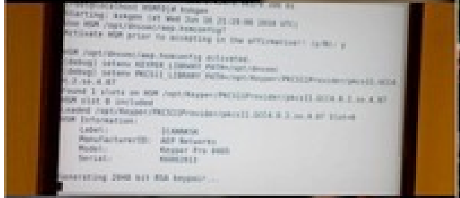
Cont…

- Got global buy in
- Direct stakeholder participation in key management – 21 Trusted Community Representatives made up of respected members of Internet community from 17 countries
  - Currently: URUGUAY, BRAZIL, TRINIDAD AND TOBAGO, CANADA, BENIN, SWEDEN, NEPAL, NETHERLANDS, NEW ZEALAND, RUSSIAN FEDERATION, PORTUGAL, JAPAN, MAURITIUS, CHINA, BURKINA FASO,CZECH REPUBLIC, UNITED KINGDOM, USA

Cont….

- Enabled DNSSEC deployment throughout hierarchy – need just one key to validate all
- Publish, broadcast everything.
- Pass 3rd party annual SysTrust audit
- ICANN Secure Key Management Facilities in Culpepper, VA and El Segundo, CA. FIPS 140-2 Level 4 crypto, GSA Class 5 safes, multiple tiers, biometrics, etc.

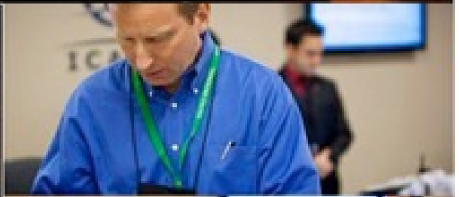
NOTICE
ALL EMPLOYEES AND VISITORS MUST WEAR IDENTIFICATION BADGES
NOTICE
NOTICE
UNAUTHORIZED PERSONS NOT PERMITTED BEYOND THIS POINT
NOTICE
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT



```
Starting: kregen (at Wed Jun 16 21:29:00 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4
0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper Pro 0405
    Serial:           K6002013

Generating 2048 bit RSA keypair...
```



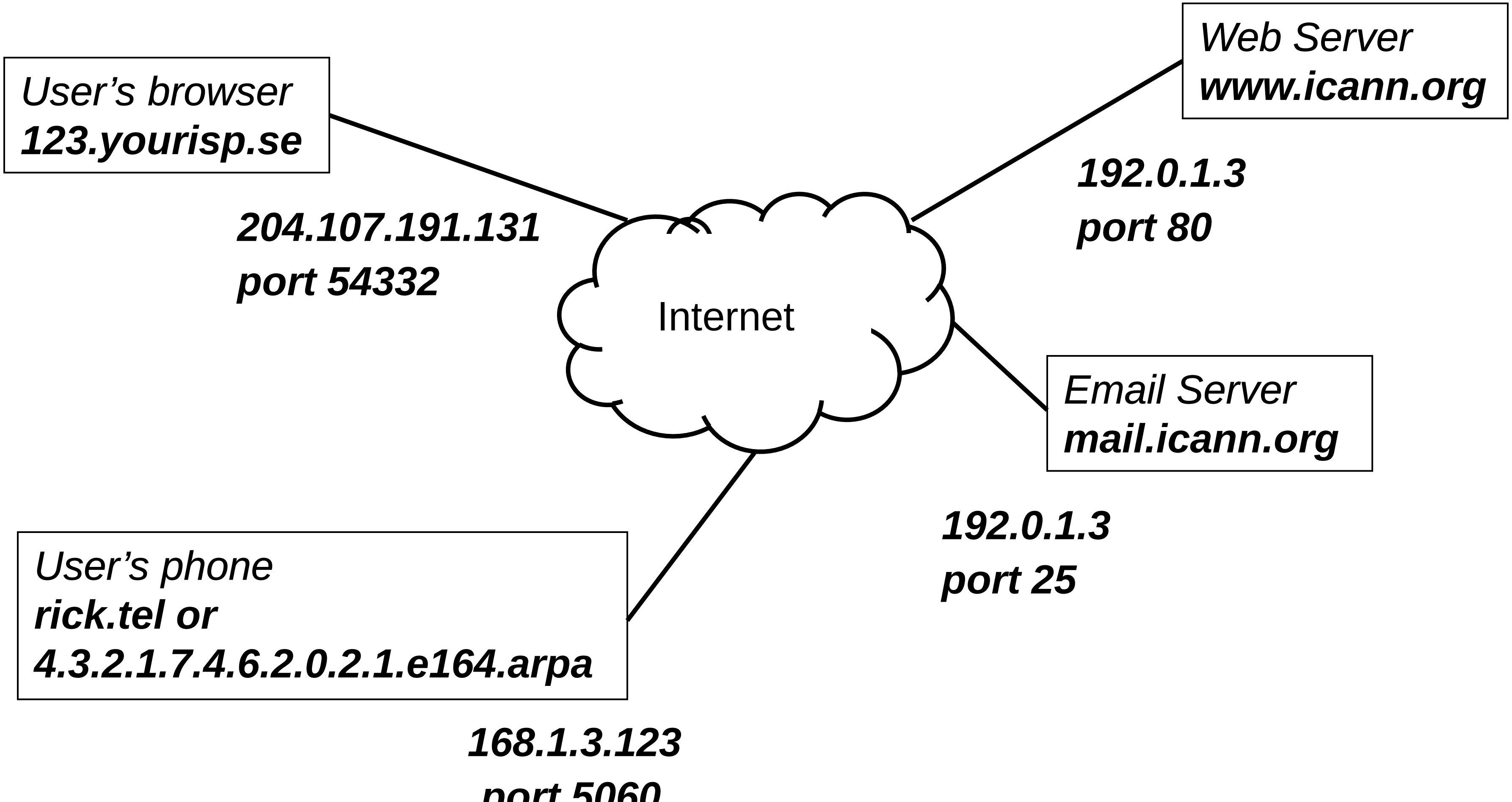
ICANN

- ICANN is a global organization that coordinates the Internet's unique identifier systems for worldwide public benefit, enabling a single, global interoperable Internet.

- ICANN's inclusive multi-stakeholder model and community-developed policies facilitate billions of computers, phones, devices and people into one Internet.

- ICANN's mission is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular, to ensure the stable and secure operation of the Internet's unique identifier systems. (Source: ICANN Bylaws as amended 25 January 2011)

IP addresses, Domain names, Parameters



User's browser
123.yourisp.se

204.107.191.131
port 54332

Web Server
www.icann.org

192.0.1.3
port 80

Internet

Email Server
mail.icann.org

192.0.1.3
port 25

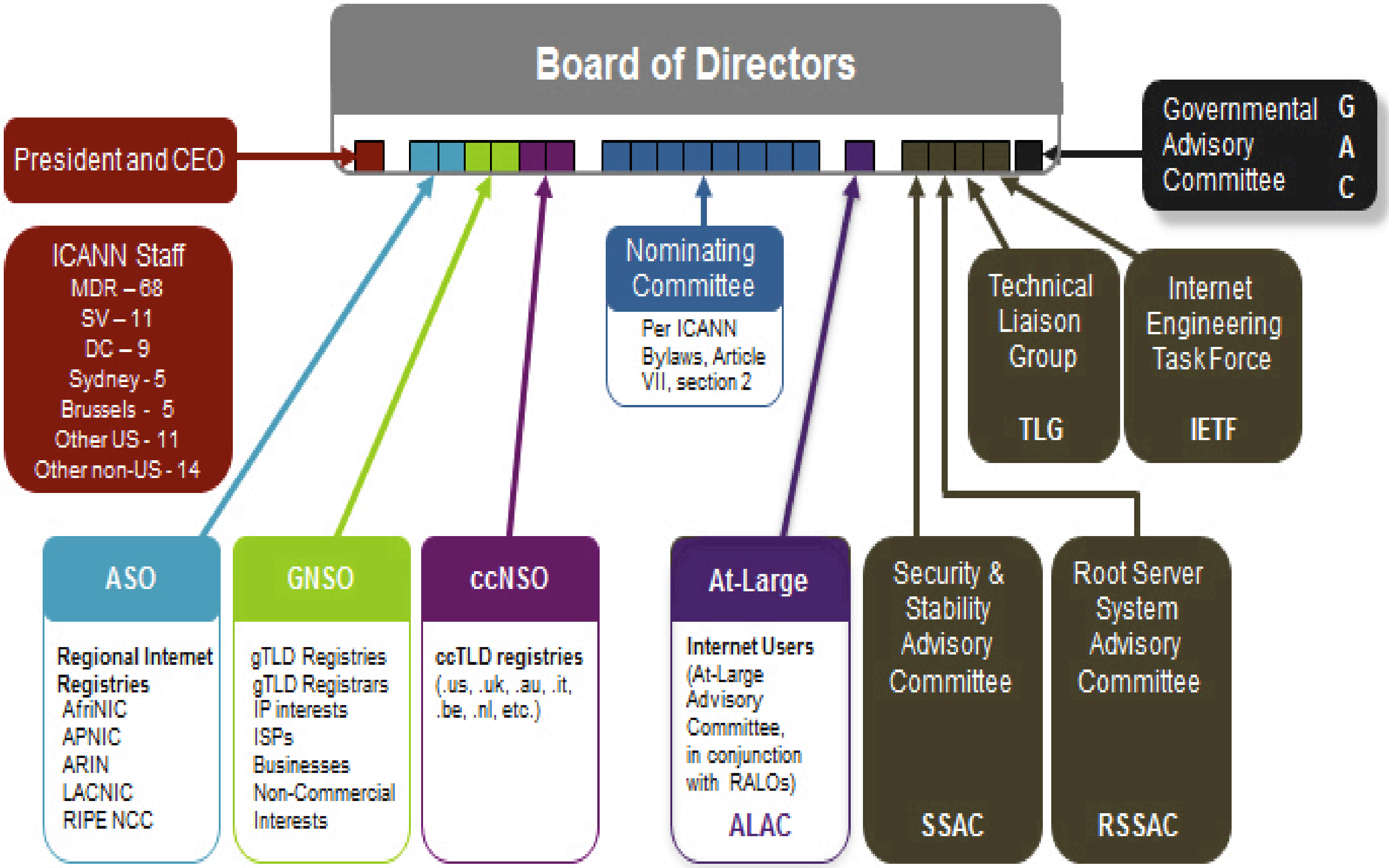
User's phone
rick.tel or
4.3.2.1.7.4.6.2.0.2.1.e164.arpa

168.1.3.123
port 5060

Background

- Created 1998 to continue technical IANA coordination function (previously performed by Jon Postel) on behalf of USG
- MoU with US DoC: ICANN will operate "in a bottom up, consensus driven, democratic manner."
- 2009 AoC: transitions U.S. oversight authority to ICANN’s Governmental Advisory Committee (GAC) and establishes accountability “review teams”
- IANA Function contract still in place

ICANN Multi-Stakeholder Model



Board of Directors

President and CEO

ICANN Staff
MDR – 68
SV – 11
DC – 9
Sydney - 5
Brussels - 5
Other US - 11
Other non-US - 14

Governmental Advisory Committee
GAC

Nominating Committee
Per ICANN Bylaws, Article VII, section 2

Technical Liaison Group
TLG

Internet Engineering Task Force
IETF

ASO
Regional Internet Registries
AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC

GNSO
gTLD Registries
gTLD Registrars
IP interests
ISPs
Businesses
Non-Commercial Interests

ccNSO
ccTLD registries (.us, .uk, .au, .it, .be, .nl, etc.)

At-Large
Internet Users (At-Large Advisory Committee, in conjunction with RALOs)
ALAC

Security & Stability Advisory Committee
SSAC

Root Server System Advisory Committee
RSSAC

What ICANN does NOT do

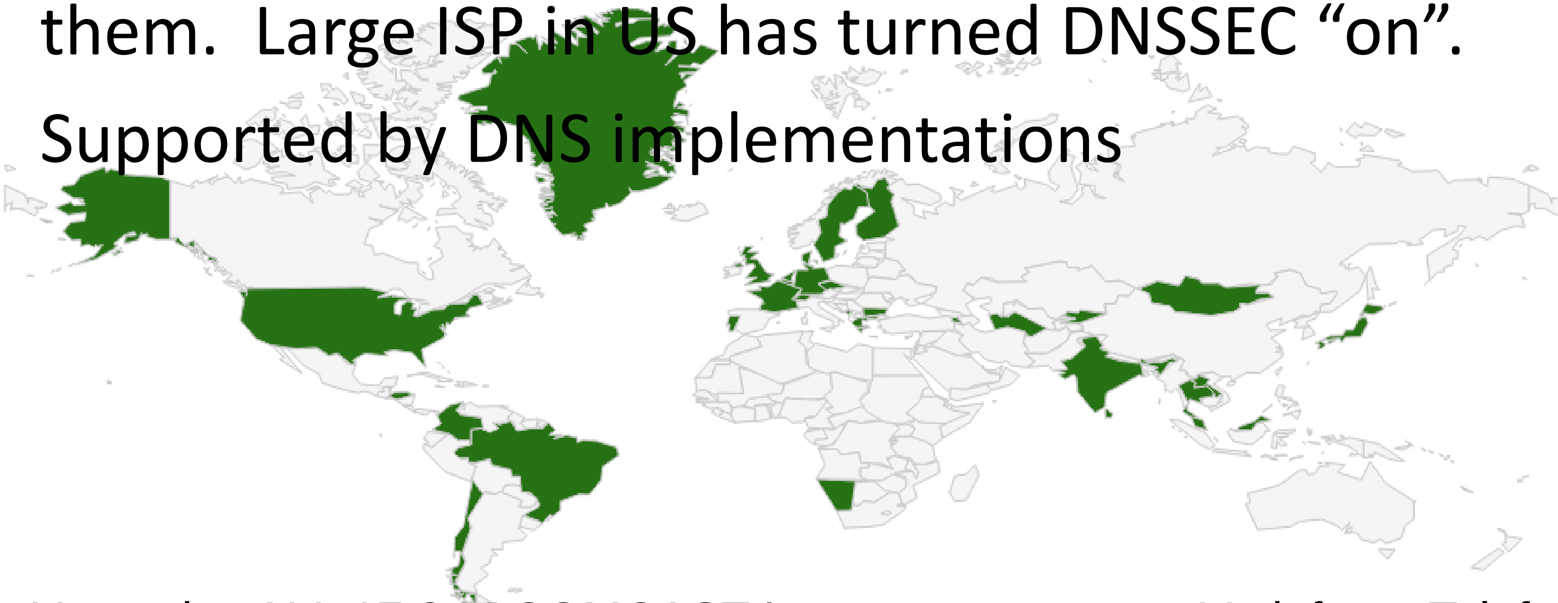
- ICANN does not play a role in policing the Internet or operationally combating criminal behavior.
- ICANN does not have a role in the use of the Internet related to cyber-espionage and cyber war.
- ICANN does not have a role in determining what constitutes illicit conduct on the Internet.
- ICANN IS able to enforce its contracts on registries & registrars

ICANN’s Role in DNSSEC

- Manage the root key of this hierarchy together with VeriSign (under contract with the US Department of Commerce) and trusted international representatives of the Internet community
- Process requests for additions/changes/deletions of public key and other records from Registries at the top of the DNS hierarchy (i.e., .com, .se, …etc)
- Educate and assist the Internet community regarding DNSSEC

Where we are now

- < 1% DNSSEC still needs to deployed on more domain names.
- 82/312 top level domain (e.g., .com) have DNSSEC deployed.   Multi-stakeholder managed root key.
- 82% of domain names can have DNSSEC deployed on them. Large ISP in US has turned DNSSEC "on".
- Supported by DNS implementations



Yesterday ALL 17.8 M COMCAST Internet customers. Vodafone, Telefonica CZ

What needs to still happen

- Needs to be widely deployed across the domain names
- Registrars, ISPs, and hosting providers need to support it in a trustworthy fashion
- DNSSEC validation needs to be pushed to the end user
- Raise awareness of the security benefits of DNSSEC and its secure deployment.

How to implement DNSSEC?

For Companies:

- Deploy DNSSEC on corporate DNS infrastructure (turn DNSSEC validation “on”)
- Deploy DNSSEC on your domain names (“sign” your corporate domain names)

For Users:

- Ask your ISP about DNSSEC (get DNSSEC validation turned “on” on their DNS servers)

Are we done?

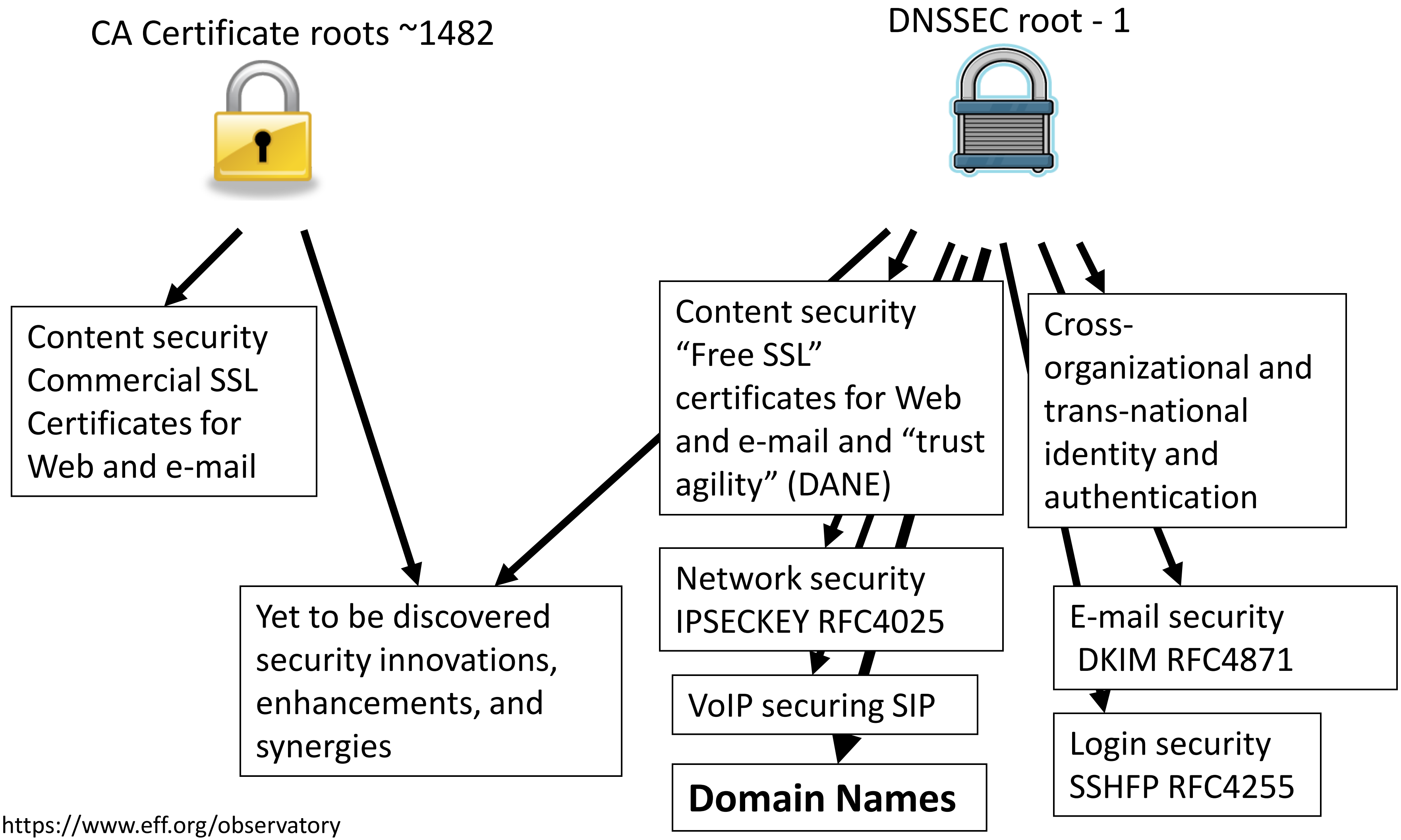
But wait, there’s more…

“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 16 June 2010 Root Key Ceremony

Cont…

- Looks like we now have a global, secure database for “free”!
- A globally trusted Public Key Infrastructure
- Enabler for global security applications
- An authentication platform for identification
- Cross-organizational and trans-national
- .. A global platform for innovation

Expect: SSL, E-mail, secured VOIP… (e.g. DANE, S/MIME, DKIM, IPSEC)



CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Yet to be discovered
security innovations,
enhancements, and
synergies

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility” (DANE)

Network security
IPSECKEY RFC4025

VoIP securing SIP

Domain Names

Cross-
organizational and
trans-national
identity and
authentication

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/

Potential Applications

- Build and improve on established trust models, e.g., CAs
- Greatly expanded SSL usage (currently ~4M/200M)
- Make SMIME a reality
- May work in concert with in enhancing or extending other cyber security efforts like digital Identities, WebID, BrowserID, CAs, ..
- Securing VoIP
- Simplify WiFi roaming security
- Secure distribution of configurations (e.g., blacklists, anti-virus sigs)

lamb@xtcn.com

mydomainname.com

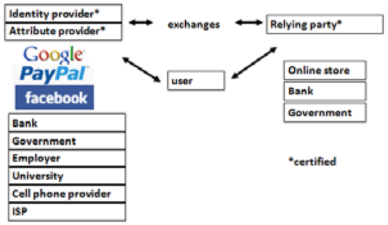
+1-202-709-5262
tel number

2001:470:8165:1:1e6f:65ff:fe87:54
IPV6

ICAO
e-Passport symbol

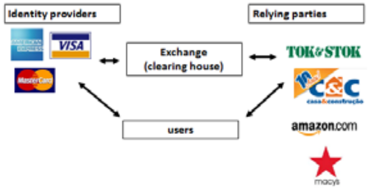
facebook
PayPal
carte d'assurance maladie
MasterCard
5412 3390 0000 1513
LEE M CARDHOLDER
MASTERCARD
PLATINUM
ELECTRONIC USE ONLY
Google
OpenID
RSA SecurID
159 759
VASCO
554322
PASSPORT
COUNTRY
ICP Brasil
O Brasil na era da certificação digital
DIRECTIVE 1999/93/EU
RFID
FEDERAL BRIDGE CERTIFICATION AUTHORITY
ACCESS WITH TRUST
General
Details
Certification Path
Certificate Information
Armed Forces of the United States
Navy
Active Duty
Parker IV, Christopher J.
E5
P02
2000SEP19
2003SEP18
Geneva Conventions Identification Card
SVERIGE SWEDEN SUÈDE
SVENSK/SWE
REPÚBLICA FEDERATIVA DO BRASIL
O chip permitiria o armazenamento de dados sobre o cidadão
O Registro de Identidade Civil seria um número nacional de identificação
FERNANDA CARVALHO DA SILVA
0000000001-9
EESTI VABARIIK
MÄNNIK
MARI-LIIS
SPECIMEN
IDUT012
SILVA<<CARVALHO<FERNANDA<<<<<<

In Search of Trust: a Perfect Storm?



- Government digital identity efforts
  - US National Strategy for Trusted Identities in Cyberspace (NSTIC) (Apr 2011), Sweden e-ID, Brazil, etc..
  - Interoperability / Assurance / Certification

Trust frameworks are not new



- Certification Authority fix /w dnssec
  - Not perfect but decades of experience: Use it!
  - Recent impetus to improve.

COMODO
Creating Trust Online®

DigiNotar®
A VASCO COMPANY

- Smart Electrical Grid efforts
  - Not just reading meters
- DNS/DNSSEC part of all ecosystems

[NSTIC http://www.nist.gov/nstic](http://www.nist.gov/nstic)

Summary

- DNSSEC will be a critical tool in combating the global nature of cyber crime allowing cross-organizational and trans-national authentication
- As a global security federation DNSSEC is a platform for cyber security innovation and international cooperation
- Successful Internet example of bottom up development and multi-stakeholder, public-private cooperation
- DNSSEC does not solve all the ills of the Internet but can become a powerful tool in improving the security of the Internet.