DNSSEC: A game changing example of multi-stakeholder cooperation

ICANN Meeting, Singapore

21 June 2011

richard.lamb@icann.org

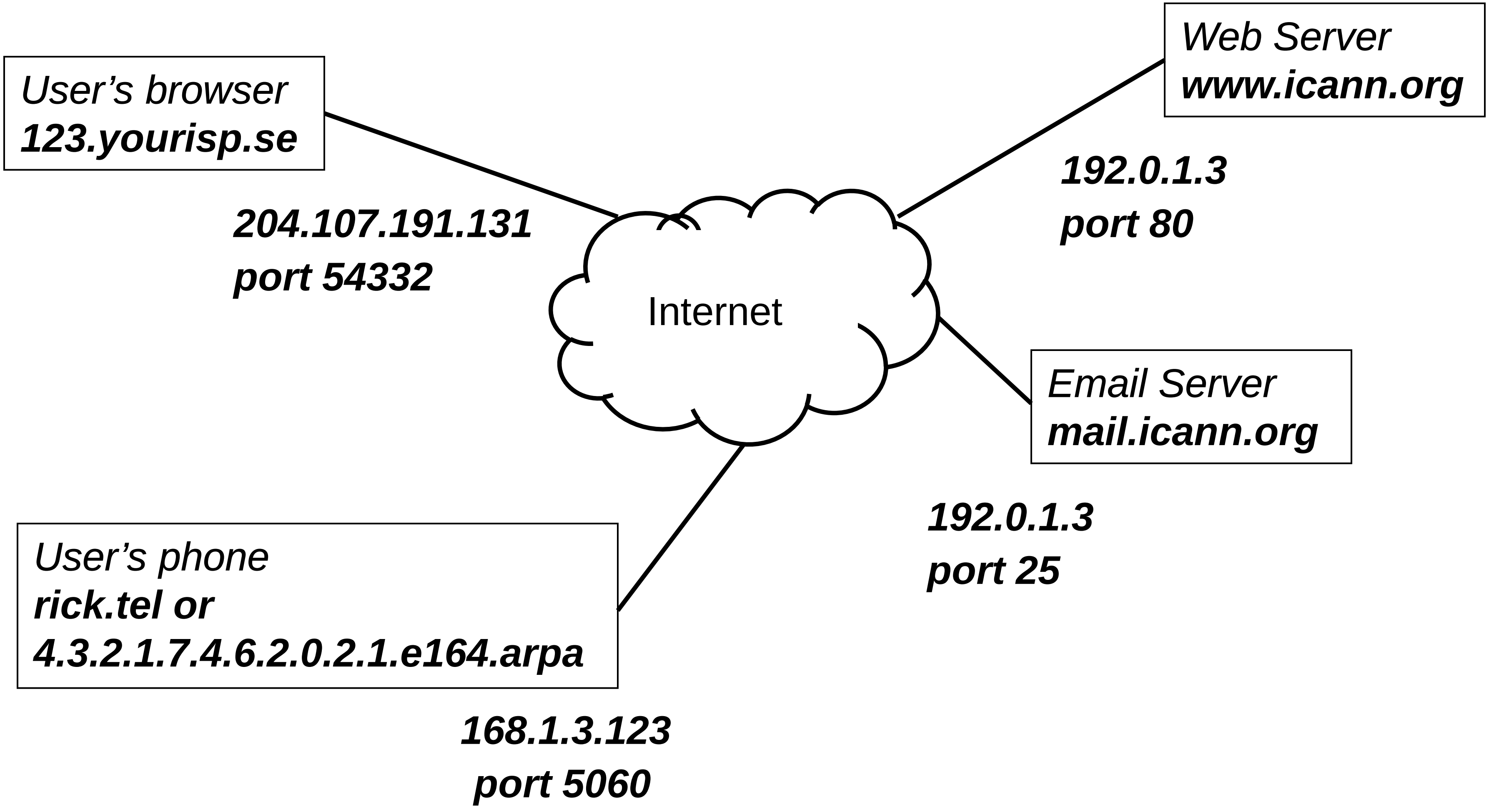
ICANN

- 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: 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

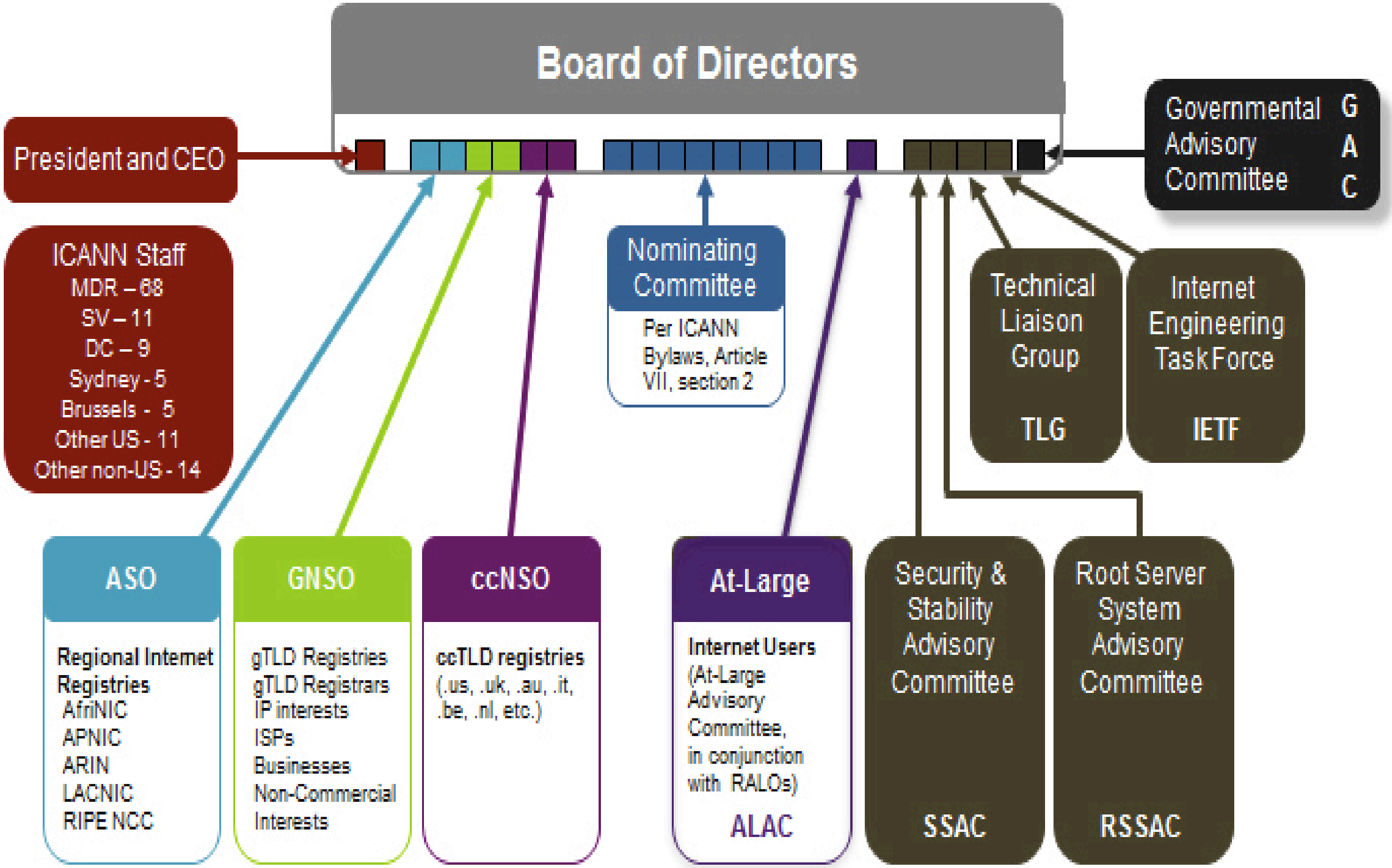
Role in the Internet ecosystem

The Internet has thrived as an ecosystem engaging many stakeholders organizing through collaboration to foster communication, creativity and commerce in a global commons.

The interoperability of the global commons depends on the operation and coordination of the Internet's unique identifier systems.

ICANN and the operators of these systems acknowledge that maintaining and enhancing the security, stability and resiliency of these systems is a core element of their collaborative relationship.

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
G
A
C

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.

…continued

- ICANN is not
  - A law enforcement agency
  - A court of law
  - Government agency
- ICANN cannot unilaterally
  - Suspend domain names
  - Transfer domain names
  - Immediately, terminate a registrar’s contract (except under limited circumstances)
- ICANN is able to enforce its contracts on registries & registrars

Current Hot Topics

- gTLDs – New global Top Level Domains
- IDN – Internationalized Domain Names
- IPv6
- DNSSEC

DNSSEC at the root

- Deployed 15 July 2010
- Set the stage for deployment in rest of hierarchy (e.g., top level domains, end user domains)
- Enabling step for global security applications
- With strong community support, it is being vigorously deployed around the world. (currently deployed on 70 / 310 top level domains including .com, .co, .cl, .br, .gov, …)

DNSSEC at the root – a classic example of bottom up Internet development and successful public-private partnership

- Based on over 15 years of global technical community development (in IETF) after discovery of vulnerability
- Deployed at root after calls from global community:
  - Internet community (e.g., RIPE, APNIC, …)
  - Governments
  - Business (e.g., Kaminsky 2008)

Cont…

- Cooperative effort with US Department of Commerce and VeriSign
- Direct stakeholder participation in management – 21 Trusted Community Representatives made up of respected members of Internet community
    - 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…

- Results:
  - Completed in very short time frame ~2years
  - Global buy in
  - Vigorous DNSSEC deployment efforts by TLDs
  - Currently deployed on 70 out of 310 TLDs
  - International SysTrust IT certification

DNSSEC – What is it?

- Internet’s phone book (DNS) converts names into numbers, e.g., www.icann.org -> 192.0.32.7. (Actually, first org then icann.org, then www.icann.org).
- DNSSEC secures the Internet’s phone book.
- DNSSEC stands for “DNS Security Extensions.”
- Works by incorporating public key cryptography into the DNS hierarchy.
- Is the result of over a decade of community based, open standards development.

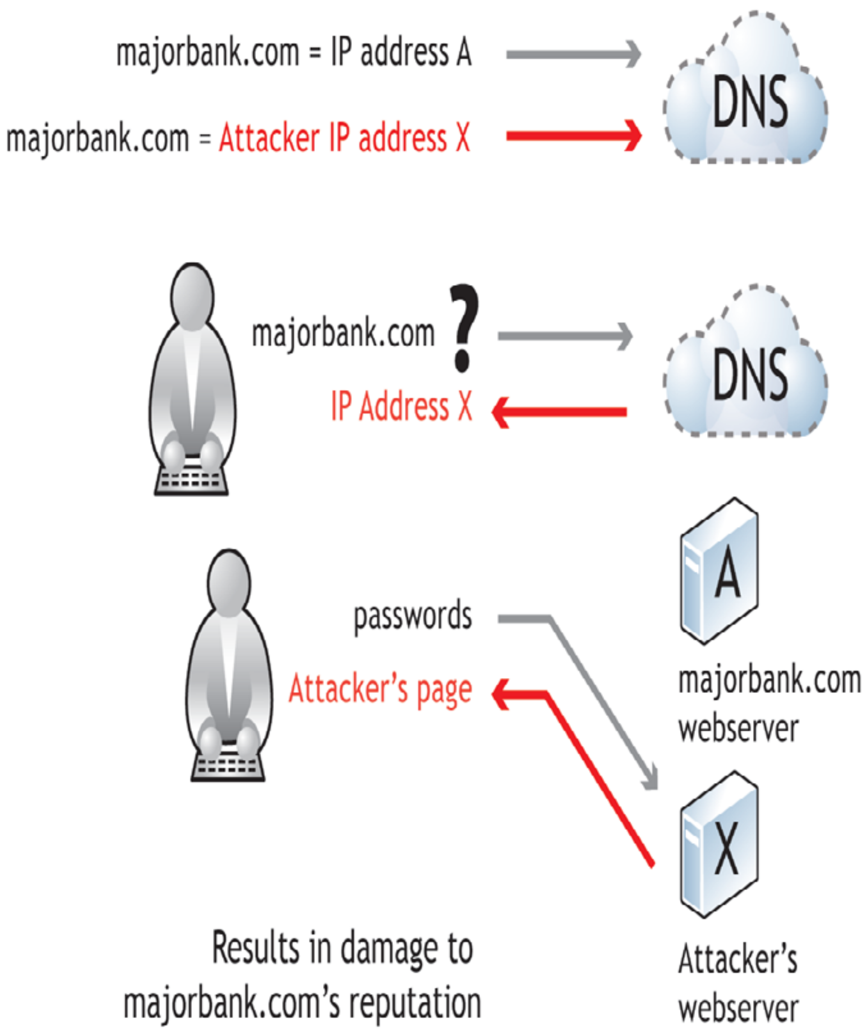
What are DNSSEC benefits?

- DNS lookup can be modified in transit to redirect an end user to an imposter or malicious site for password collection.
- Modification attacks carried out en masse at ISP/enterprise = cache poisoning.
- A lookup secured with DNSSEC is protected against modification = primary benefit.
- Greatest benefits may be yet to come.
- DNSSEC deployment at root and TLDs set the stage

DNSSEC does not solve everything

- Does not eliminate SPAM or solve phishing problem alone
- Needs to be deployed across the DNS hierarchy
- Registrars and other providers need to improve their process and practices

Without DNSSEC



majorbank.com = IP address A

majorbank.com = Attacker IP address X

DNS

majorbank.com ?

IP Address X

DNS

passwords

Attacker's page

A

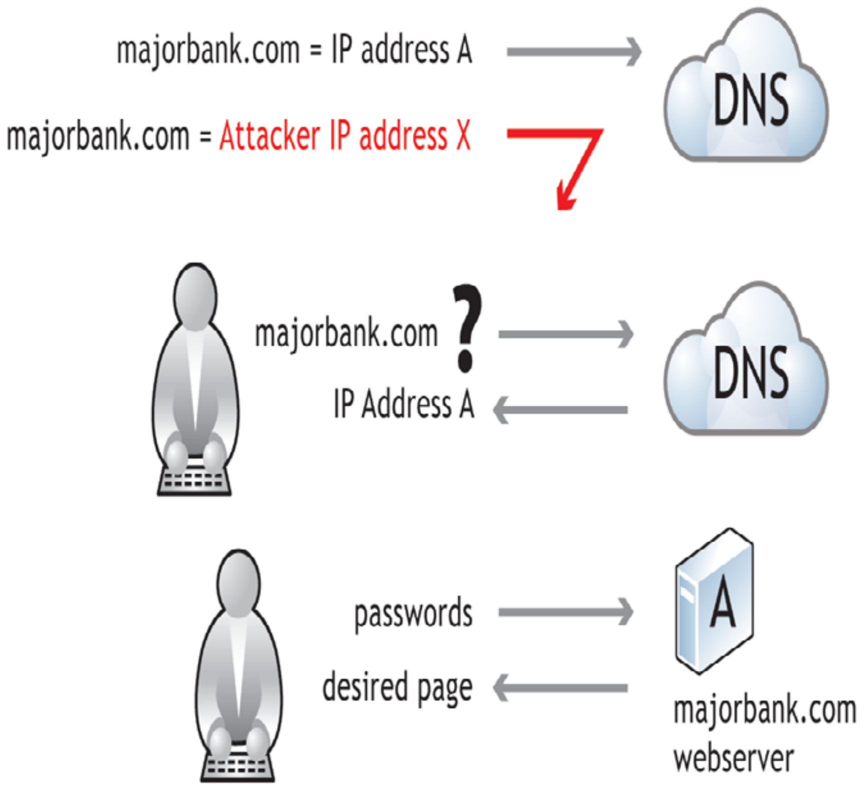
majorbank.com webserver

X

Attacker's webserver

Results in damage to majorbank.com's reputation

With DNSSEC



majorbank.com = IP address A

majorbank.com = Attacker IP address X

DNS

majorbank.com ?

IP Address A

DNS

passwords

desired page

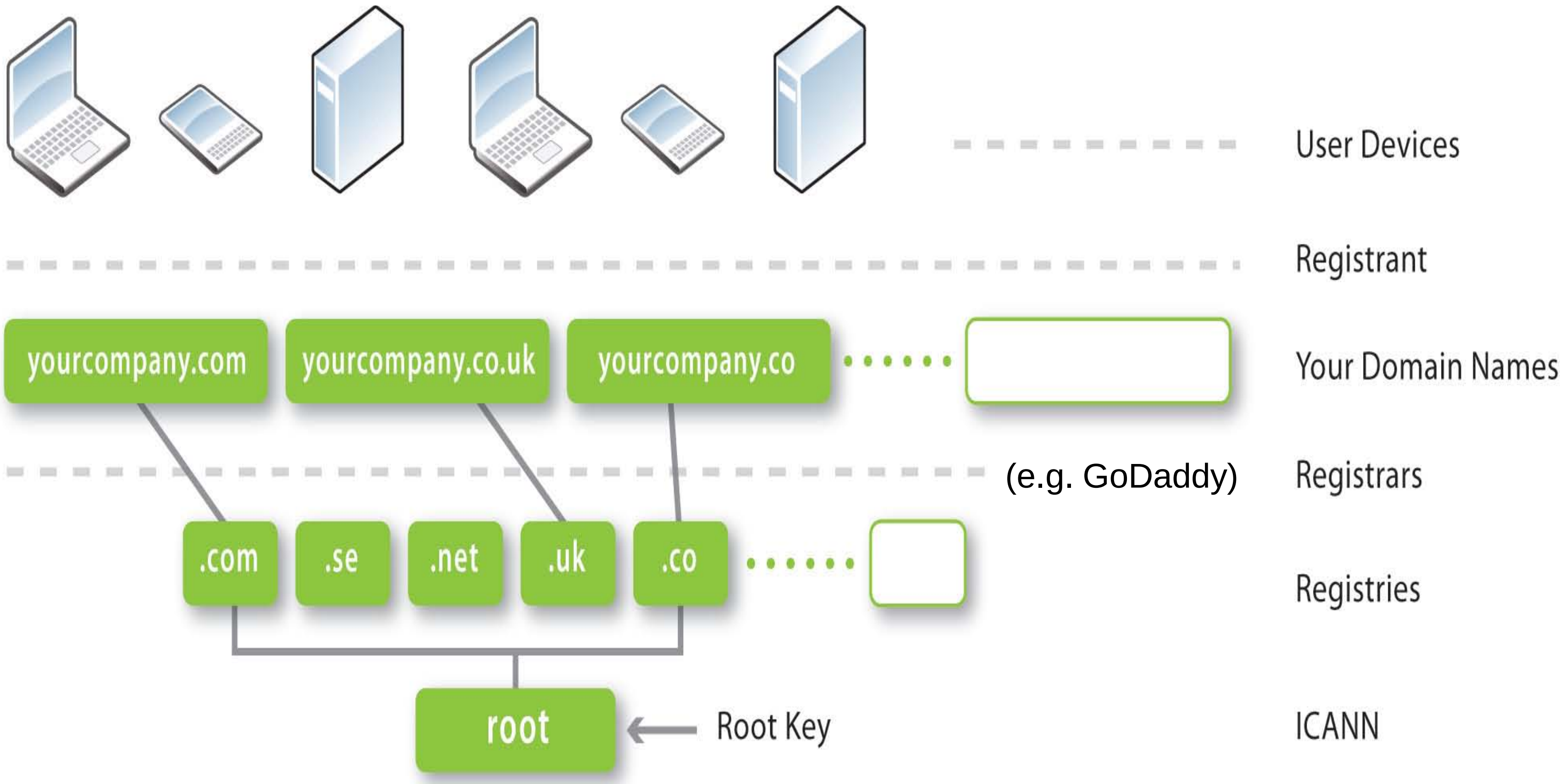
A

majorbank.com webserver

ICANN’s DNSSEC Role

- Manage the root key of this hierarchy together with VeriSign (under IANA 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, .co…)
- Educate and assist the Internet community regarding DNSSEC and its deployment

DNSSEC in the ecosystem



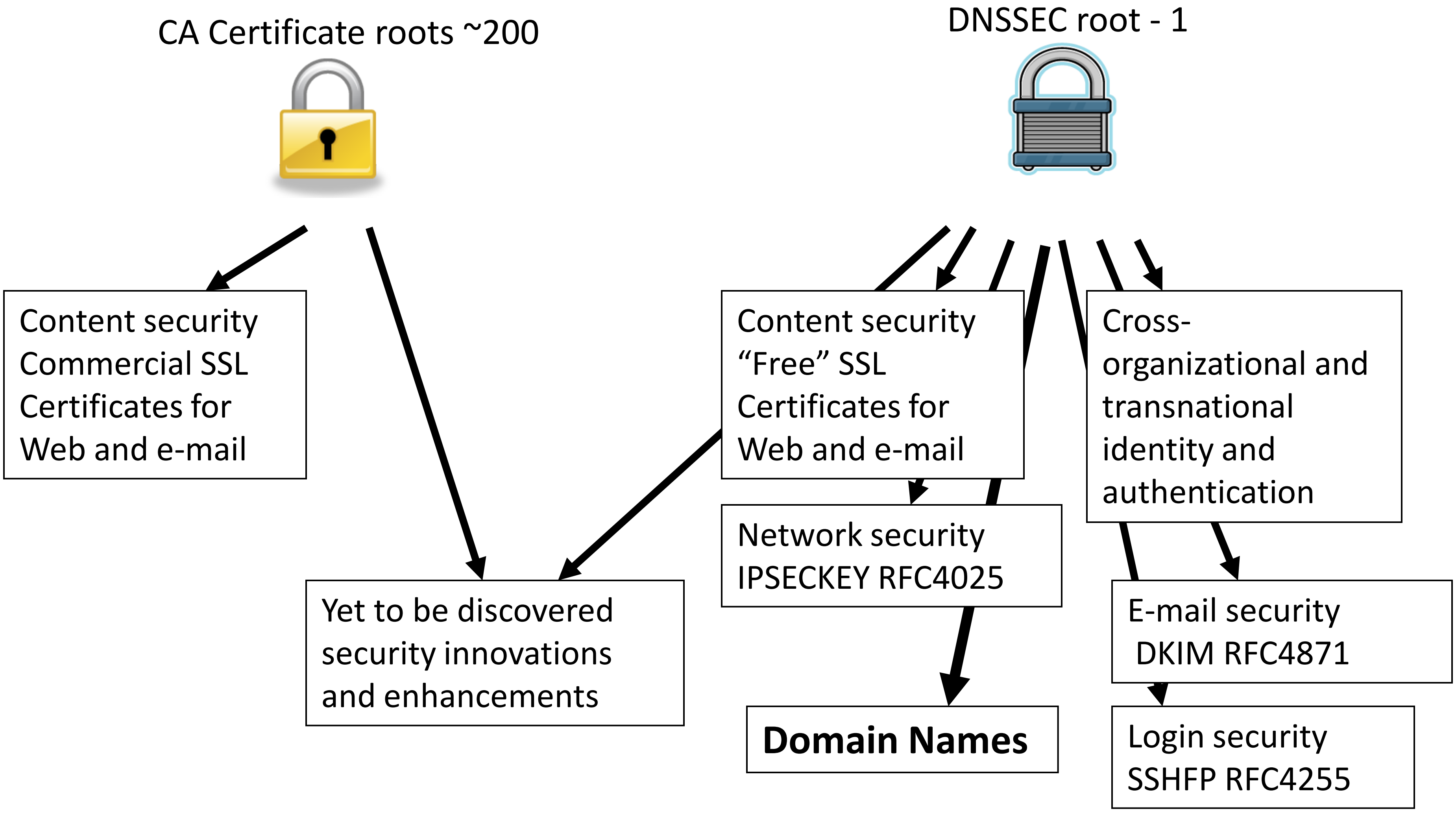
How to implement DNSSEC?

- ***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)

At root signing Vint Cerf, June 2010

“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. And so I would predict that although we started out putting this system together to assure that the domain name lookups return valid internet addresses, that in the long run this hierarchical structure of trust will be applied to a number of other functions that require strong authentication. And so you will have seen a new major milestone in the internet story.”

Opportunity (global PKI?)



CA Certificate roots ~200

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
“Free” SSL
Certificates for
Web and e-mail

Cross-organizational and transnational identity and authentication

Yet to be discovered security innovations and enhancements

Network security
IPSECKEY RFC4025

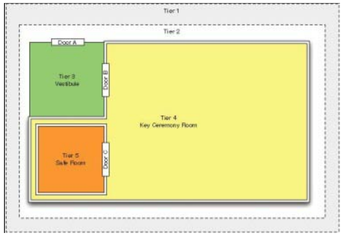
E-mail security
DKIM RFC4871

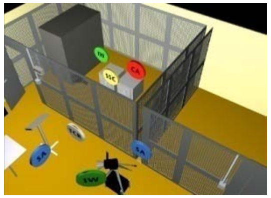
Domain Names

Login security
SSHFP RFC4255

For geeks: DNSSEC Root Details

- **Publish all material (film, scripts, s/w, results.. http://www.iana.org/dnssec)**
- **DNSSEC Practices Statement (DPS)**
- **21 global Trusted Community Representatives (TCR)**
- **3rd party SysTrust audit by PWC – success!**
- **2048 KSK, 1024 ZSK RSA keys; SHA256 hash**
- **FIPS 140-2 Level 4 HSM; 3-of-7 TCR to enable; Good RNG**
- **Multiple physical tiers /w multi-person anti-passback access control system**
- **9 gauge stretched metal ceremony room construction;**
- **Safes certified to 20 hours surreptitious entry**
- **24x7 monitoring: motion, seismic, video, guards**
- **~60 day window to perform quarterly operation; 15 day signature validity**
- **Mirror sites in Los Angeles and Washington DC; 2 HSMs at each site**
- **Documented Disaster Recovery (DR) plans**
- **Incremental deployment with DURZ and extensive monitoring**
- **Carefully scripted Key Ceremonies**





Where we are now

- Accelerating DNSSEC Deployment
  - Collaboration with industry resulted in secure and free system with no lock in for ccTLDs [1]
  - Requirements for new gTLDs
  - ..and the rest of the 200M+ domain names
- Industry has stepped up with multiple solutions (e.g. , $2/domain/year [2])
- ICANN and other organizations (e.g., ISOC, RIRs, ccTLD groups) offering training and best practices to Registries and Registrars to improve processes and practices.
- RPKI for protecting IP addressing/routing – Like DNSSEC working with NRO/RIR organizations to manage root key

[1] http://svsf40.icann.org/meetings/siliconvalley2011/presentation-cctld-dnssec-signing-platform-16mar11-en.pdf

[2] http://svsf40.icann.org/meetings/siliconvalley2011/presentation-verisign-16mar11-en.pdf

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 public-private sector cooperation
- Many solutions exist to ease DNSSEC deployment

Thank You!

Questions?