DNSSEC and ICANN

15 March 2011

richard.lamb@icann.org

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.
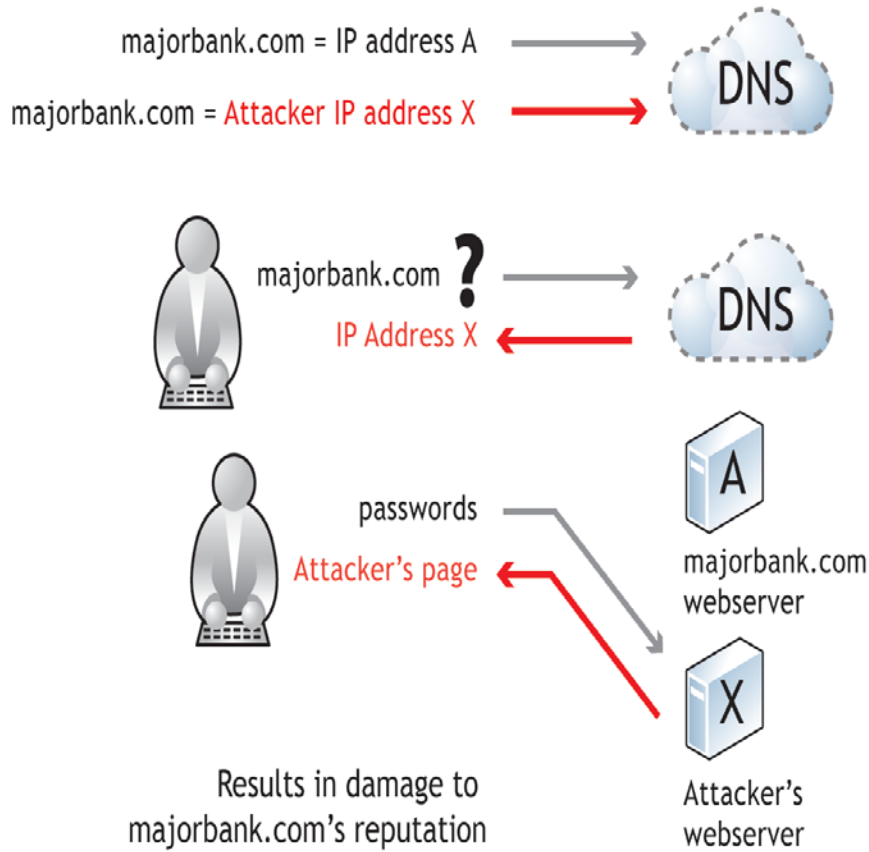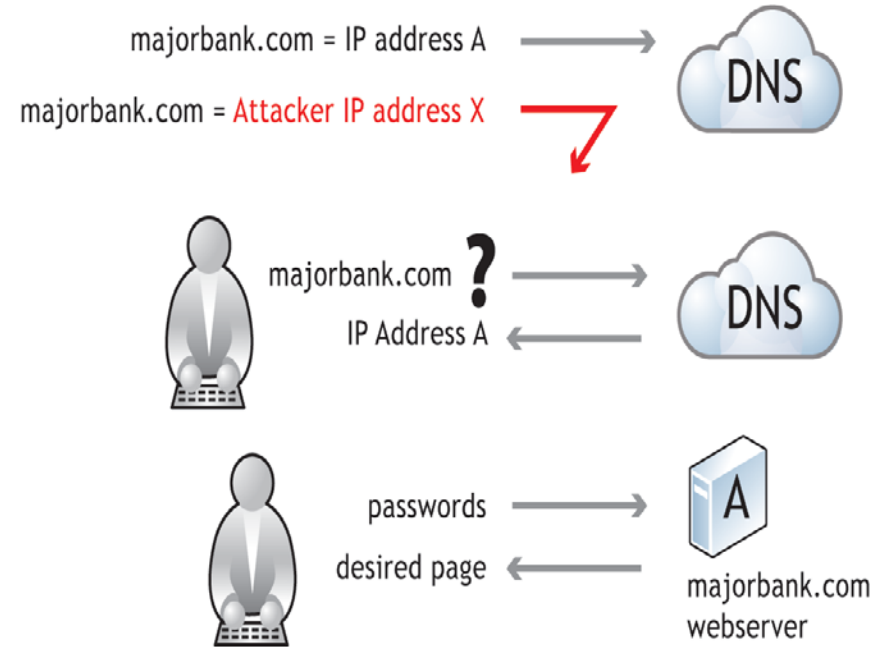
What are DNSSEC benefits?

• 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 (though not encrypted) = primary benefit.

• Greatest benefits may be yet to come. Why not securely distribute more than just DNS info? Other keys? Identification info?

• You know, DNS has No boundaries.

• DNSSEC deployment at root and TLDs set the stage

Without DNSSEC

majorbank.com = IP address A

majorbank.com = Attacker IP address X

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

majorbank.com **?**
IP Address A

DNS

passwords
desired page

A
majorbank.com
webserver

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)
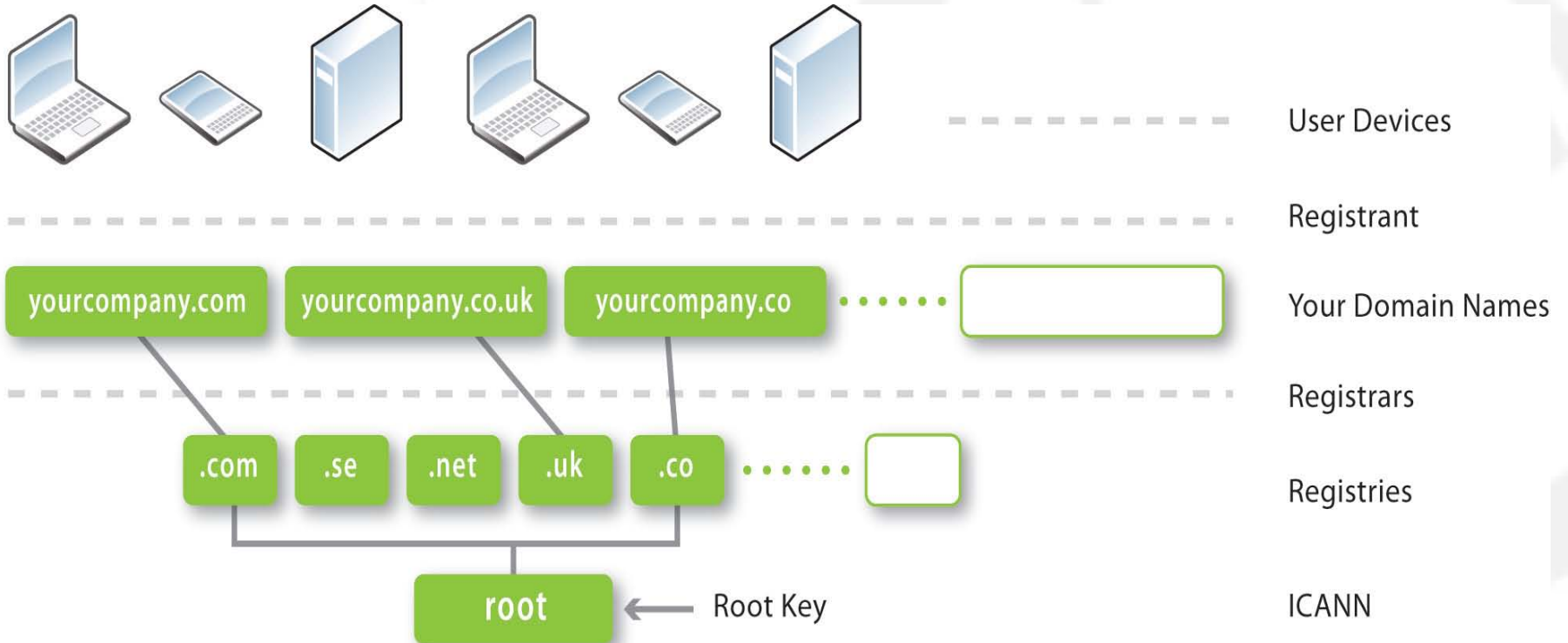
ICANN's Role

- 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

In the Ecosystem

User Devices

Registrant

Your Domain Names

Registrars

Registries

ICANN

yourcompany.com   yourcompany.co.uk   yourcompany.co

.com   .se   .net   .uk   .co

root ← Root Key

ICANN Community Groups involved in DNSSEC

• Commercial Stakeholders Group (CSG)

• Commercial and Business Users Constituency (BC)

• Internet Service providers and Connectivity Providers Constituency (ISPCP)

• Non-Commercial Stakeholders Group (NCSG)

• Non-Commercial Users Constituency (NCUC)

• Security and Stability Advisory Committee (SSAC)

• Country Code Names Supporting Organization (ccNSO)

For Technical Advice

- IETF http://www.ietf.org,

    http://tools.ietf.org/pdf/draft-ietf-dnsop-rfc4641bis-05.pdf

- DNSSEC Deployment Initiative

    http://www.dnssec-deployment.org

- ISC http://www.isc.org

- NLNETLABS http://www.nlnetlabs.nl

- DNSSEC.NET http://www.dnssec.net

One World

One Internet

Questions