



CARIBBEAN **ICT** Roadshow

Overview of DNSSEC

17 January 2012

Roseau Dominica

richard.lamb@icann.org



Caribbean
Telecommunications
Union

ICT Innovation for
Caribbean **DEVELOPMENT**

- 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.

Recent News

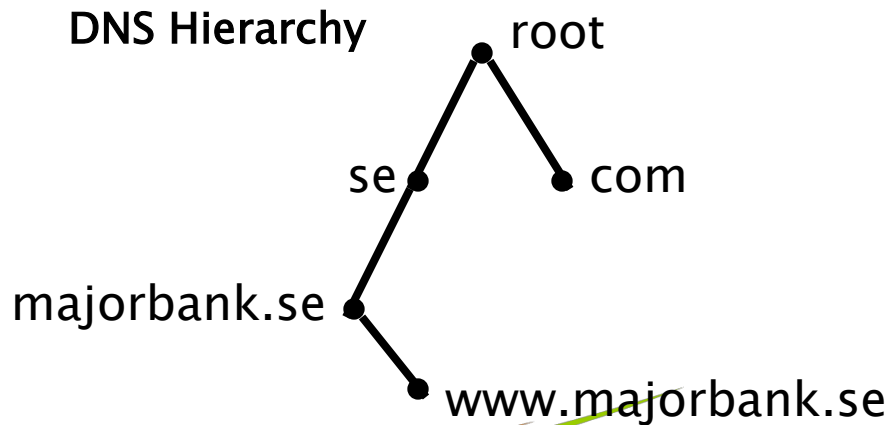
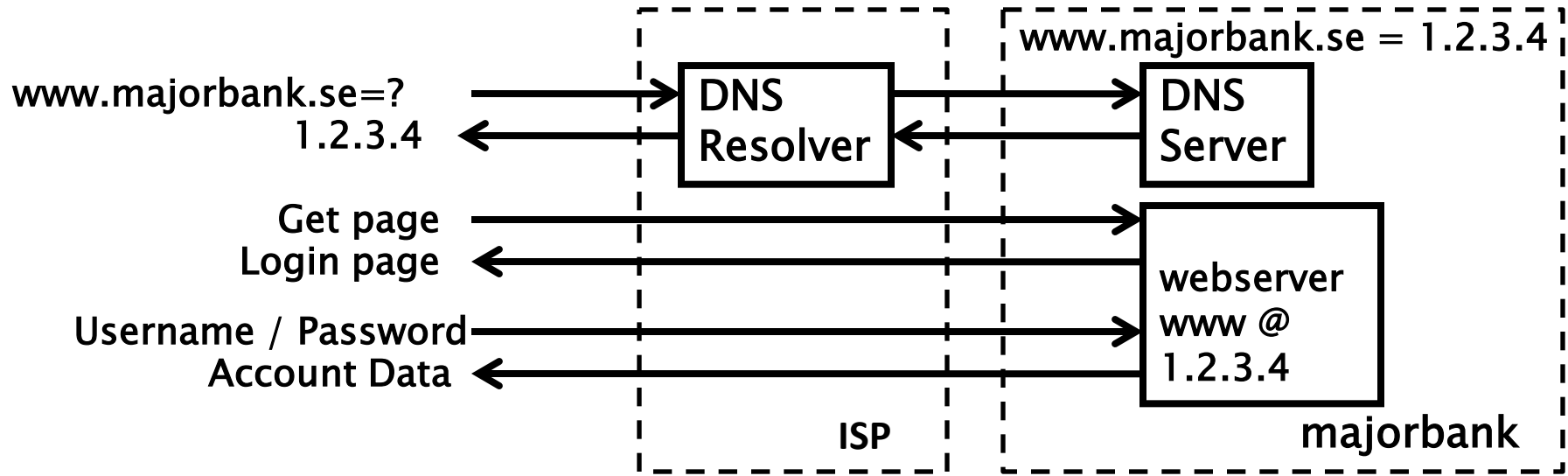
- 9 Nov 2011 - DNSChanger/Ghost Click: 4M PCs across 100 countries
- 7 Nov 2011 - Large scale Brazilian ISP DNS poisoning attack
- 3 Aug 2008 - Dan Kaminsky reveals DNS cache poisoning shortcut
- Highlights need for securing DNS

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

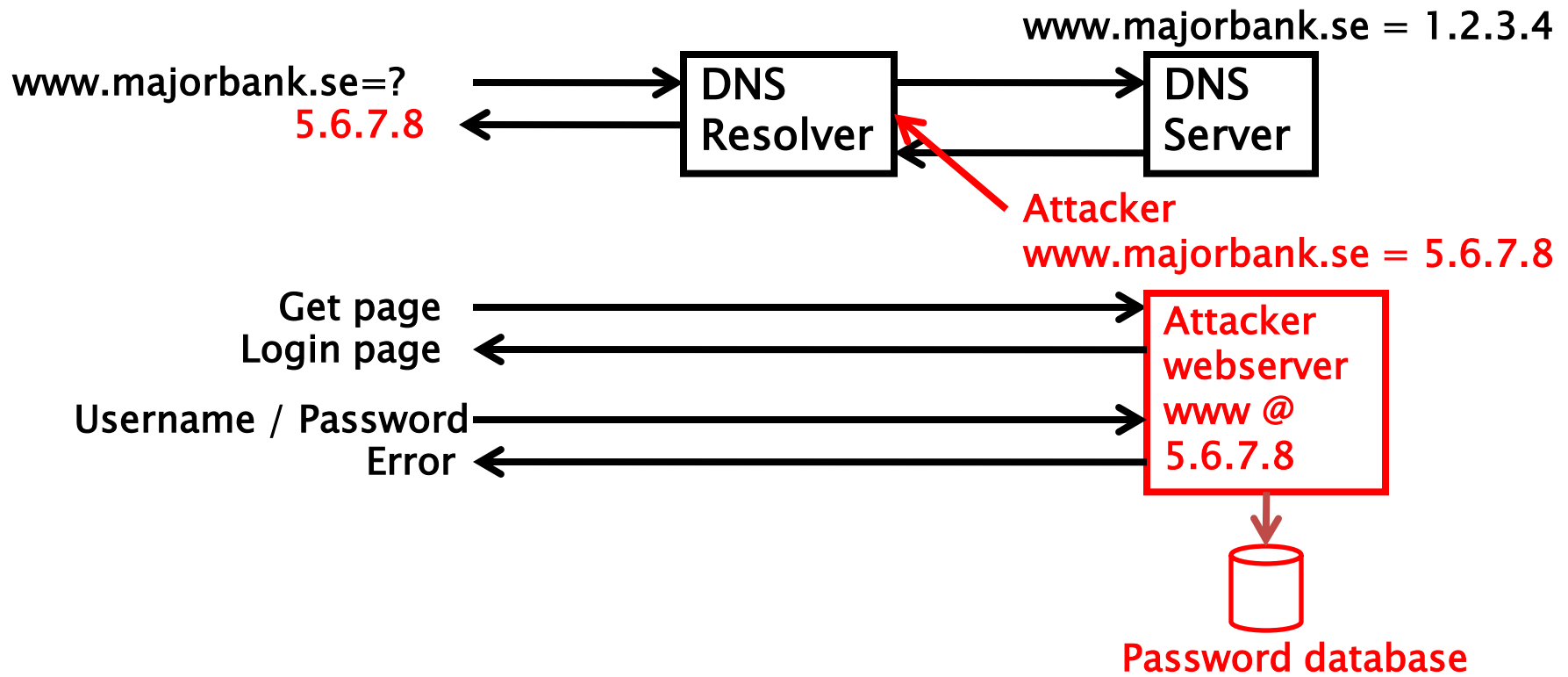
[http://www.securelist.com/en/blog/208193214/Massive DNS poisoning attacks in Brazil](http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil)

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

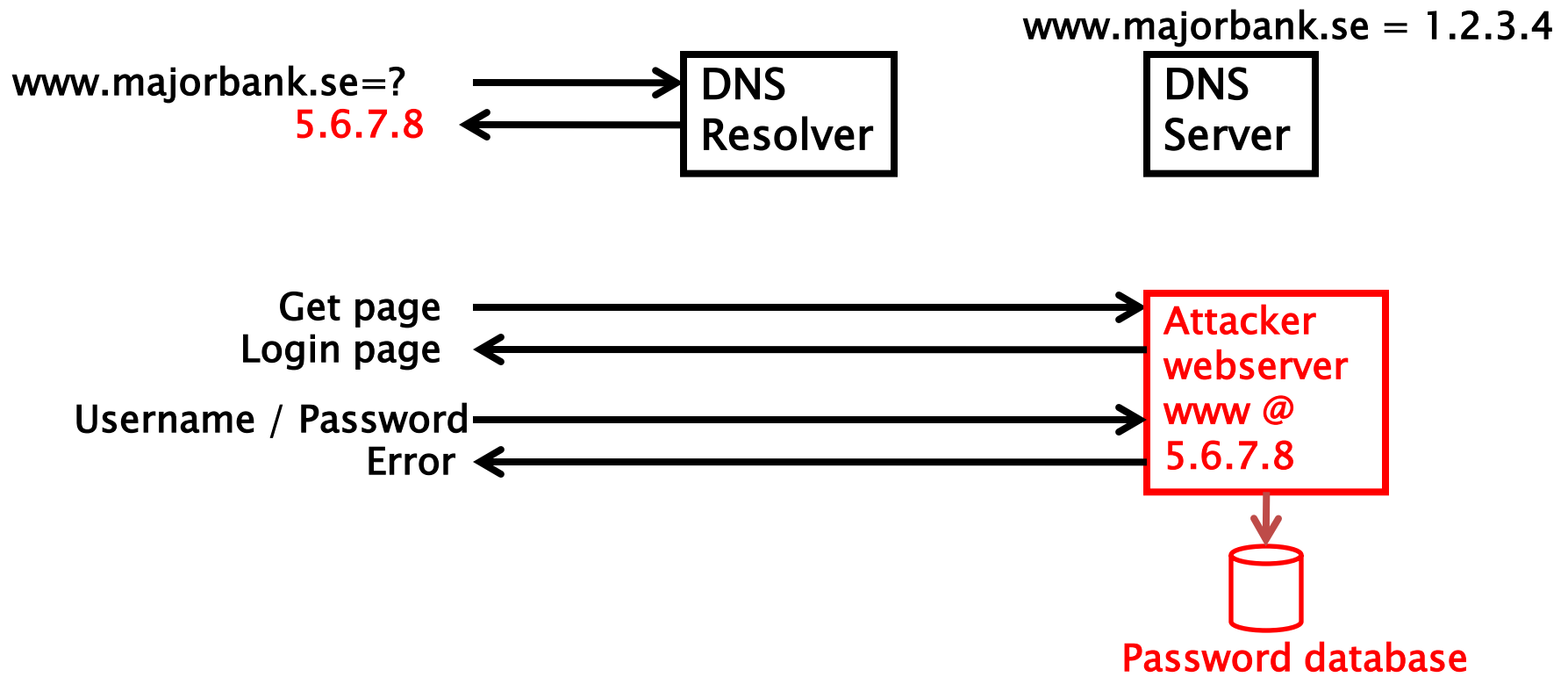
The Internet's Phone Book - Domain Name System (DNS)



The Problem: DNS Cache Poisoning Attack

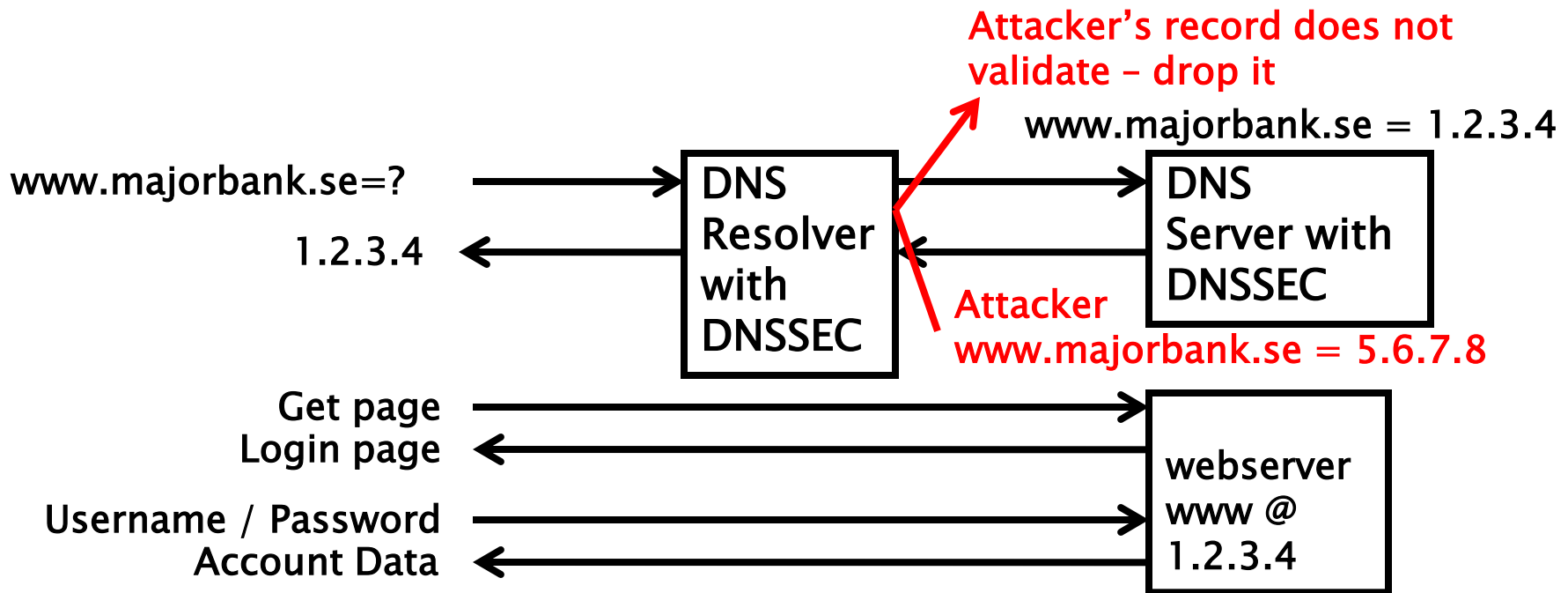


Argghh! Now all ISP customers get sent to attacker.

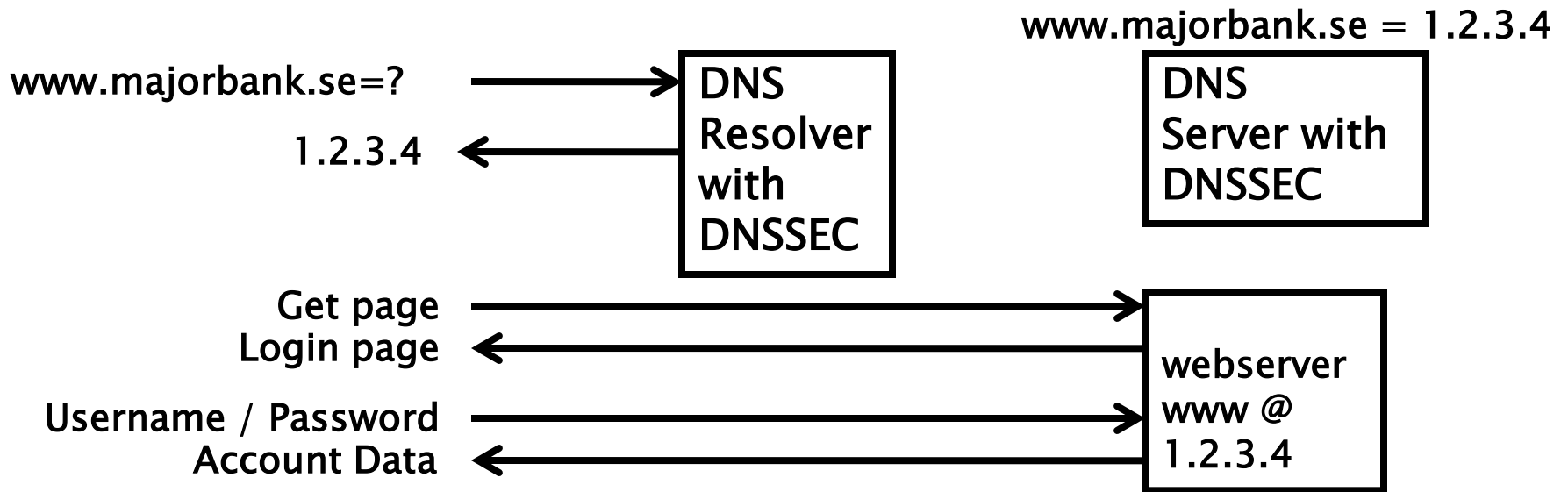


Securing The Phone Book - DNS Security Extensions (DNSSEC)

- Add keys to hierarchy; 15+ years of standards work; backwards compatible

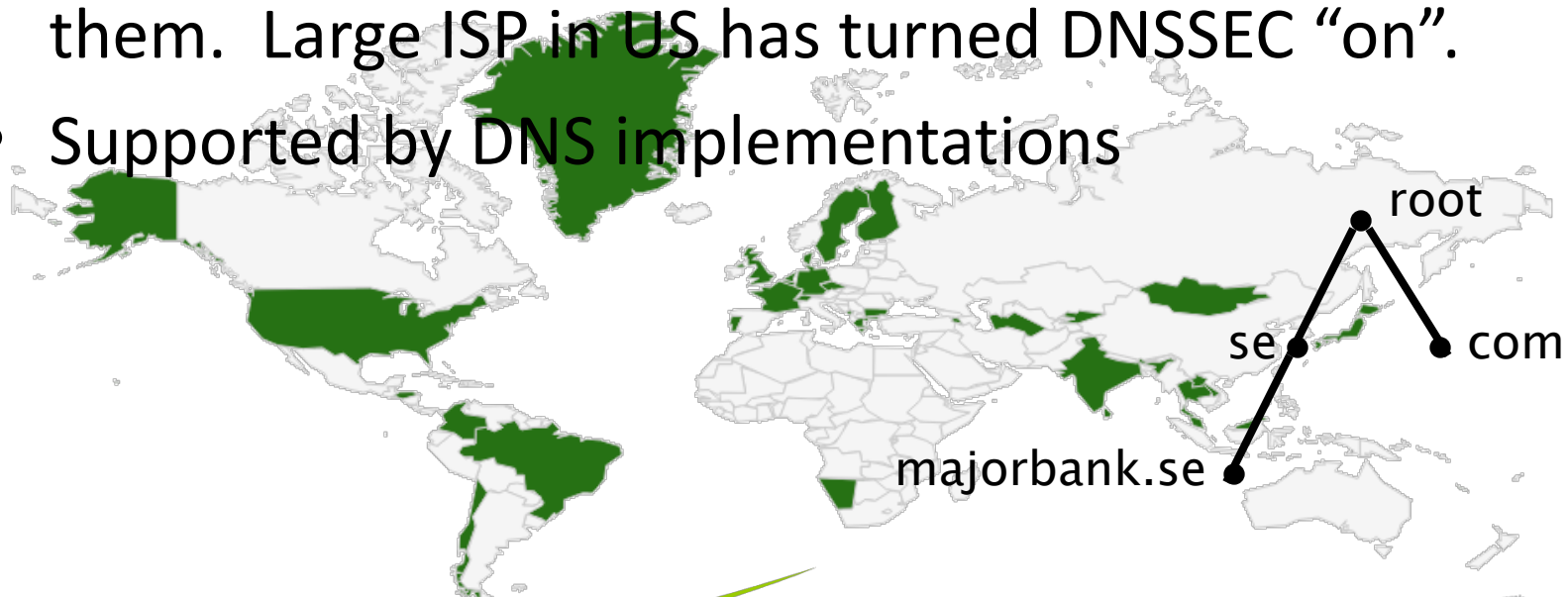


Resolver only caches validated records



DNSSEC Deployment: Where we are now

- < 1% DNSSEC still needs to be deployed on more domain names.
- 82/312 top level domain (e.g., .se) 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



Last week ALL 17.8 M COMCAST Internet customers. Vodafone, Telefonica CZ

Deploying DNSSEC at the top (root)

An International Multi-Stakeholder, Bottom-up, Cooperative effort

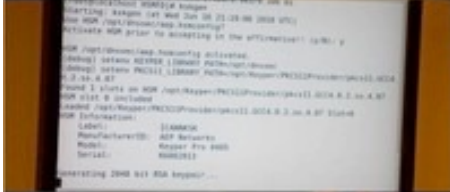
- **Bottom-up:** Responding to calls for deployment at root by Internet Community, IT security researchers, and Governments. Based on 15+ years of development in IETF and experience from early deployments by ccTLDs (SE, BR, PR, etc..).
- **Multi-Stakeholder:** “root signed” 15 July 2010 and managed with direct participation by 21 respected Internet representatives from 17 countries.
- **Transparent:** We publish and broadcast everything and have annual 3rd party audit.



Result

- Biggest upgrade to the Internet's core infrastructure in 20 years
- Enabled DNSSEC deployment throughout hierarchy
- Who is this guy?





How to implement DNSSEC?

- ***For Companies:***
 - Sign your corporate domain names (ask Registrars to support DNSSEC)
 - Just turn on validation on corporate DNS resolvers
- ***For Users:***
 - Ask ISP to turn on validation on their DNS resolvers
- Take advantage of ICANN and other organizations offering education and training.

But wait, there's more...

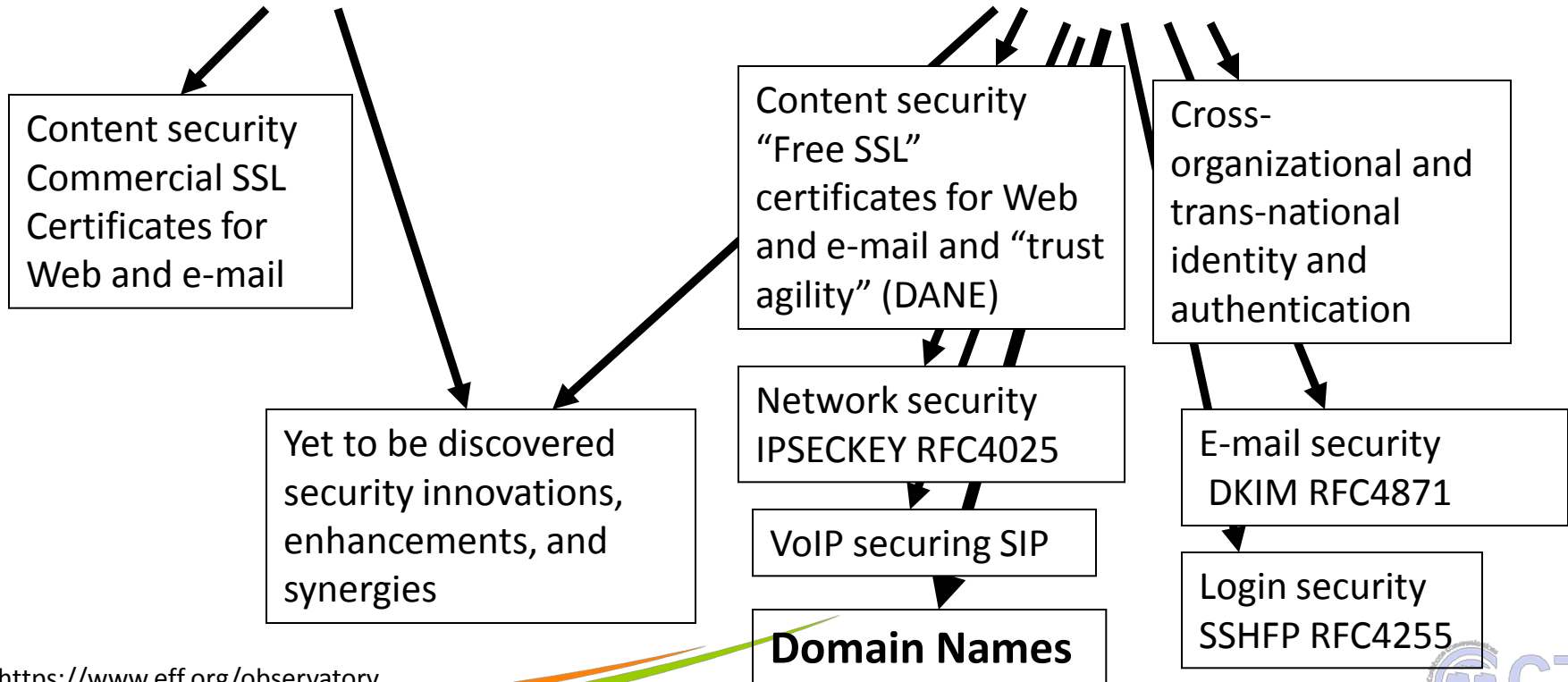
- Looks like we now have a global, secure database for “free”!
- A globally trusted Public Key Infrastructure
- Enabler for global security applications
- An authentication platform for identification
- Cross-organizational and trans-national
- .. A global platform for innovation

Another Source of Trust on the Internet

CA Certificate roots ~1482



DNSSEC root - 1



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)

Opportunity for Indigenous Certification Authorities

- CAs located in only 52 countries
 - 'AE', 'AT', 'AU', 'BE', 'BG', 'BM', 'BR', 'CA', 'CH', 'CL', 'CN', 'CO', 'CZ', 'DE', 'DK', 'EE', 'ES', 'EU', 'FI', 'FR', 'GB', 'HK', 'HU', 'IE', 'IL', 'IN', 'IS', 'IT', 'JP', 'KR', 'LT', 'LV', 'MK', 'MO', 'MX', 'MY', 'NL', 'NO', 'PL', 'PT', 'RO', 'RU', 'SE', 'SG', 'SI', 'SK', 'TN', 'TR', 'TW', 'UK', 'US', 'UY', 'WW', 'ZA'
- Even then, some countries are not using their own CAs.
- Synergy: Reduced barriers, Alignment with TLD, DNSSEC operations

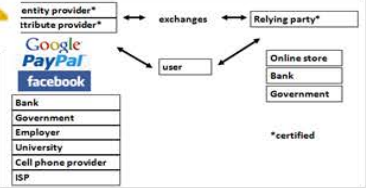
+1-202-709-5262

VoIP

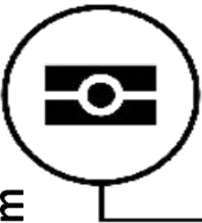
DNS is a part of all ecosystems

facebook

PayPal™



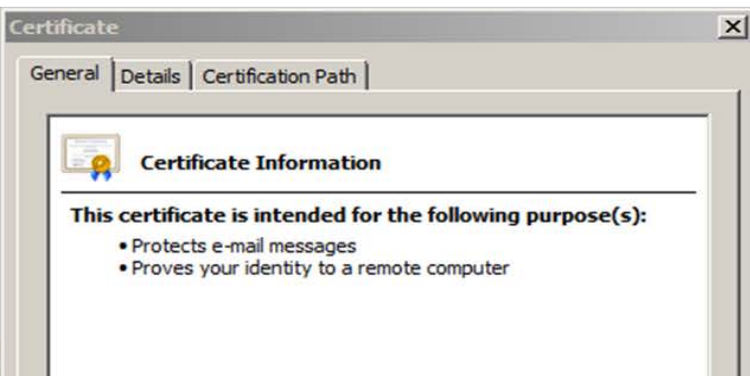
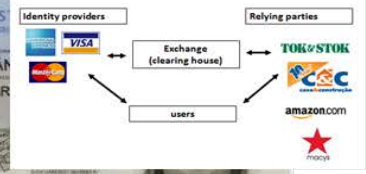
e-Passport symbol



Smart Electrical Grid

lamb@xtcn.com

Trust frameworks are not new



What needs to still happen

- Needs to be widely deployed across more 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.

Summary

- DNSSEC is a platform for cyber security innovation and international cooperation.
- DNSSEC does not solve all the ills of the Internet but can become a powerful tool in improving the security of the Internet.
- DNSSEC will be a critical tool in combating the global nature of cyber crime allowing cross-organizational and trans-national authentication.
- DNSSEC is a game changing example of what can result from the bottom-up, multi-stakeholder process the Internet has come to be known for.
- In order to realize the full benefits of DNSSEC, greater end user and domain name owner awareness is needed to drive a virtuous cycle for effective deployment.