DNSSEC Deployment: Where We Are (and where we need to be)

MENOG 10, Dubai

30 April 2012

richard.lamb@icann.org

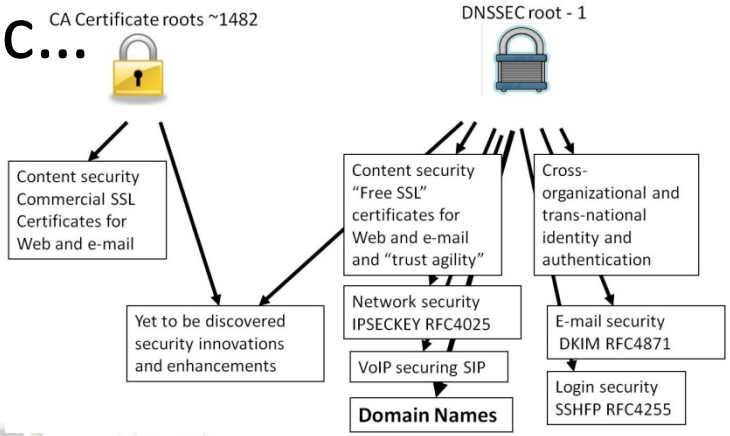
DNSSEC: We have passed the point of no return

- Fast pace of deployment at the TLD level
- Stable deployment at root

→Inevitable widespread deployment across core infrastructure

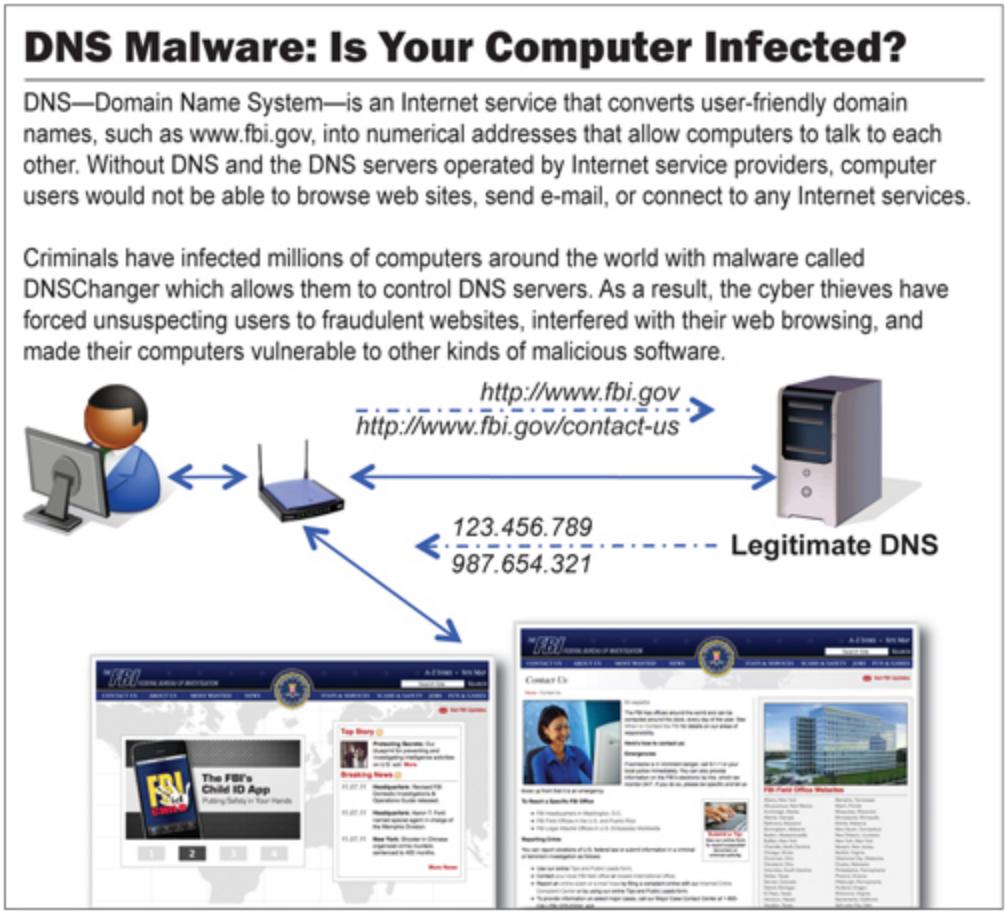
DNSSEC: Plenty of Motivation

- DNSChanger (10 Nov 2011), Brazilian ISP (7 Nov 2011), calls by government, etc…
- DANE
  - Improved Web TLS for all
  - Email S/MIME for all
- …and
  - SSH, IPSEC, VoIP
  - Digital identity
  - Other content (e.g. configurations, XML, app updates)
  - Smart Grid
  - A global PKI



http://www.internetsociety.org/deploy360/dnssec/

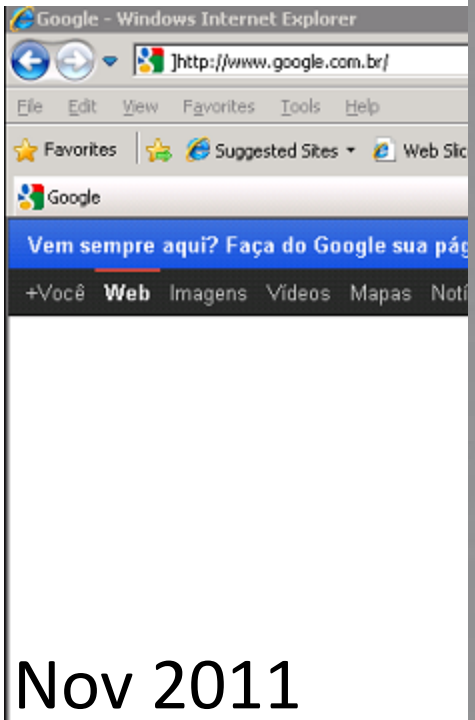
The BAD: DNSChanger - 'Biggest Cybercriminal Takedown in History' – 4M machines, 100 countries, $14M

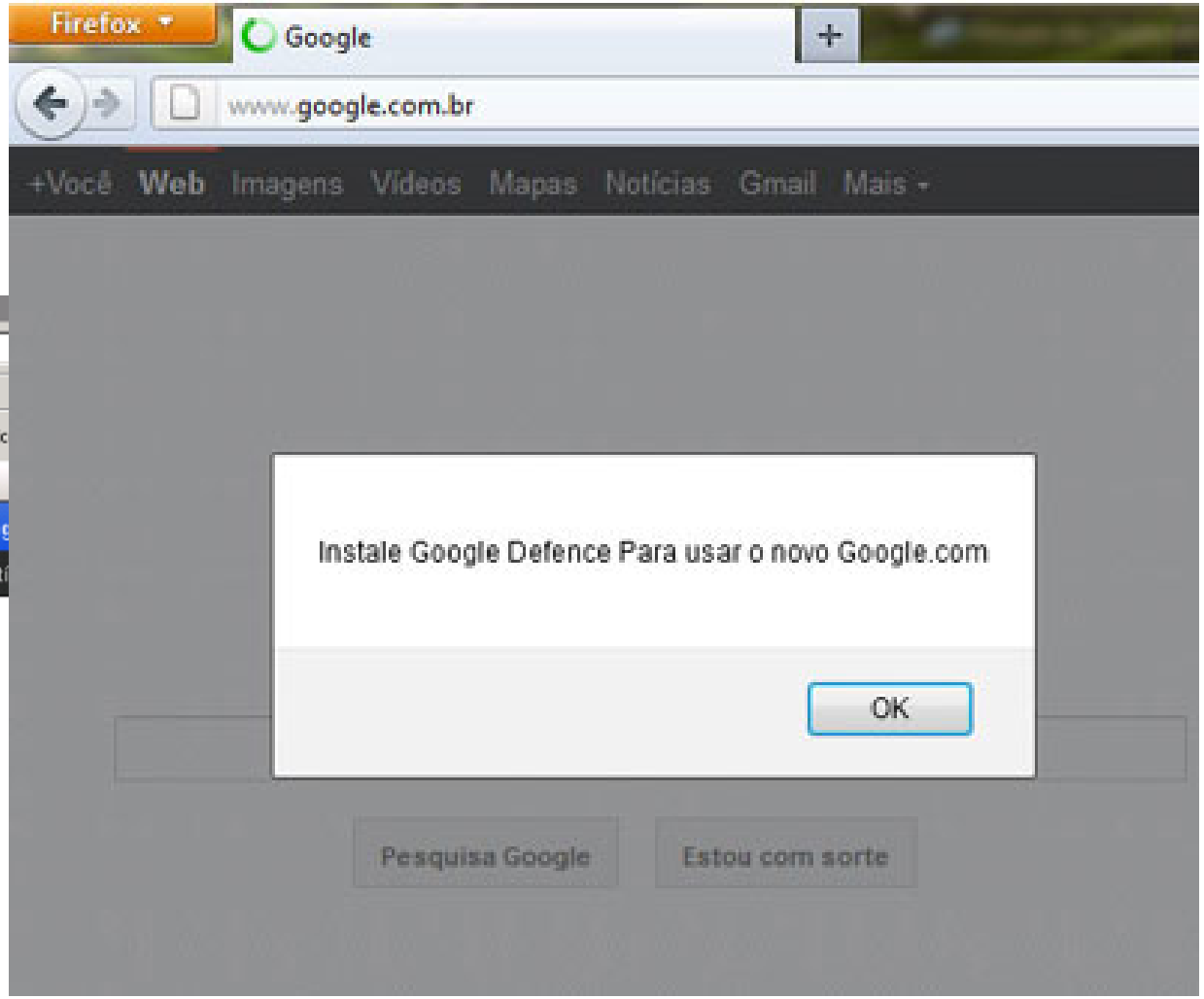


9 Nov 2011

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

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





7 Nov 2011

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

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

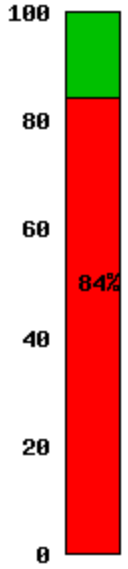
DNSSEC support from government

- Sweden, Brazil, and others encourage DNSSEC deployment
- 22 Mar 2012 - AT&T, CenturyLink, Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC recommendations .. “A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,”[1].
- 2009 .gov mandate [2]

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

DNSSEC: Where we are

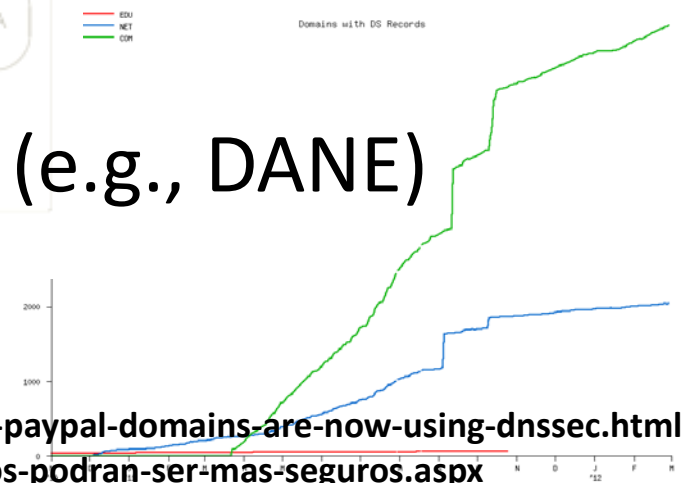
- Deployed on 86/313 TLDs (.uk, .fr, .asia, .in, .lk, .kg, .tm, .am, .tw 台灣 台湾, .jp, .cr, .com,…)
- Root signed and audited
- 84% of domain names could have could have DNSSEC deployed on them
- Large ISP has turned DNSSEC validation “on”*
- A few 3rd party signing solutions (e.g., GoDaddy, VeriSign, Binero,…)
- Unbound, BIND, DNSSEC-trigger, vsResolver and other last mile. DANE standard almost done



*Jan 2012 - 18M COMCAST Internet customers. Others..TeliaSonera SE, Vodafone CZ,Telefonica, CZ, T-mobile NL, SurfNet NL, others..

DNSSEC: Where we are

- But deployed on < 1% of 2nd level domains. Many have plans. Few have taken the step (e.g., paypal.com*).
- DNSChanger and other attacks highlight today's need.
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.

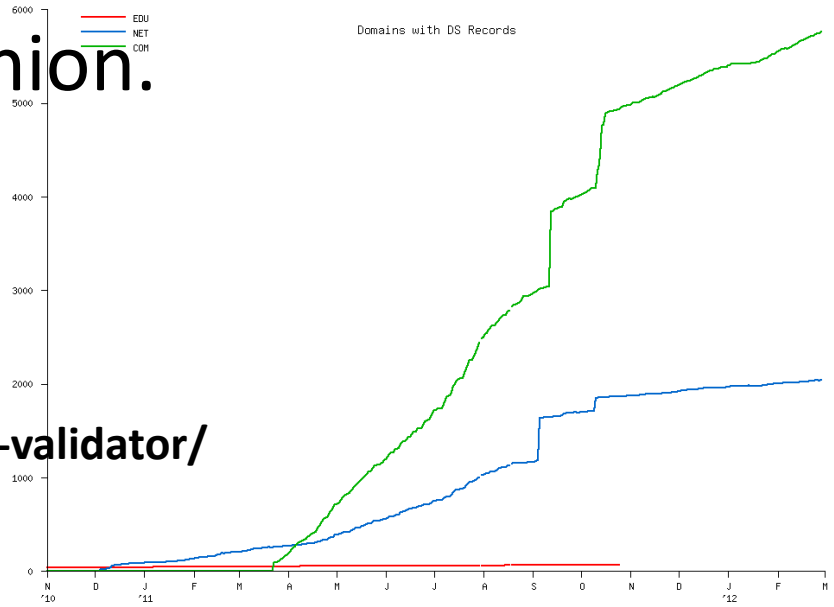


* http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html

http://www.nacion.com/2012-03-15/Tecnologia/Sitios-web-de-bancos-ticos-podran-ser-mas-seguros.aspx

What needs to happen

- ISPs need to support DNSSEC*.
- Domain name holders need to sign.
- …all in a trustworthy fashion.



*** Tools to test with https://labs.nic.cz/dnssec-validator/**

Barriers to success

- Registrar support*
  - chicken and egg
- Ease of implementation
  - security/crypto/management cost/complexity
  - no click and sign
- Trust
  - insecure practices and processes
  - garbage in, garbage out

*http://www.icann.org/en/news/in-focus/dnssec/deployment

Solutions

- Create demand for DNSSEC: Raise awareness of domain holders (content) and users (eyes)
- Ease Implementation:
  - DNSSEC training drawn from existing implementations
  - Key management automation and monitoring
  - Crypto: HSM? Smartcard? TPM chip? Soft keys? - all good
- Trust: Transparent and Secure processes and practices
  - Writing a DPS creates the right mindset for:
    - Separation of duties
    - Documented procedures
    - Audit logging
  - Opportunity to improve overall operations using DNSSEC as an excuse

Learn from CA successes (and mistakes)

- The good:
  - The people
  - The mindset
  - The practices
  - The legal framework
  - The audit against international accounting and technical standards

COMODO
Creating Trust Online®

- The bad:
  - Diluted trust with a race to the bottom (>1400 CA's)
  - DigiNotar
    - Weak and inconsistent polices and controls
    - Lack of compromise notification (non-transparent)
    - Audits don't solve everything (ETSI audit)

DigiNotar®
A VASCO COMPANY

An implementation can be thi$

…or this

FIPS 140-2 Vali

FIPS VALIDATED 140-2

The Communications Security Establishment of the Government of Canada

ive levels of security: Level 1, L
d environments in which cryptog
ign and implementation of a cry
ct identified as:

Athena IDProtect by Athen
AT90SC25672RCT Revision D;

ting accredited laboratory.

+

Level 3		
Level 3		
Level 4	Cryptographic Key Management:	Level 3
Level 3	Self-Tests:	Level 3
Level 3	Mitigation of Other Attacks:	Level 3
Level N/A	tested in the following configuration(s): N/A	

Algorithms are used: Triple-DES (Cert. #560); Triple-DES MAC (Triple-DES Cert. #560, vendor affirmed); AES (Cert. #577); SHS (Cert. #633); RNG (Cert. #332); RSA (Cert. #264)

following non-FIPS approved algorithms: RSA (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)

Overall Level Achieved: 3

Signed on behalf of the Government of the United States

Signature: William C Barker

Dated: March 31, 2008

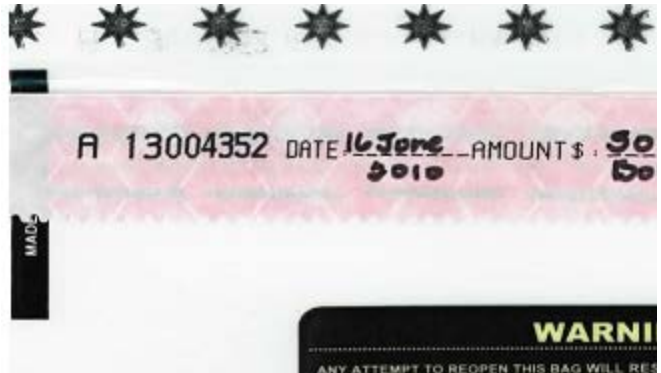
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

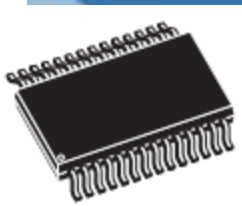
Signature:

Dated: 20 March 2008

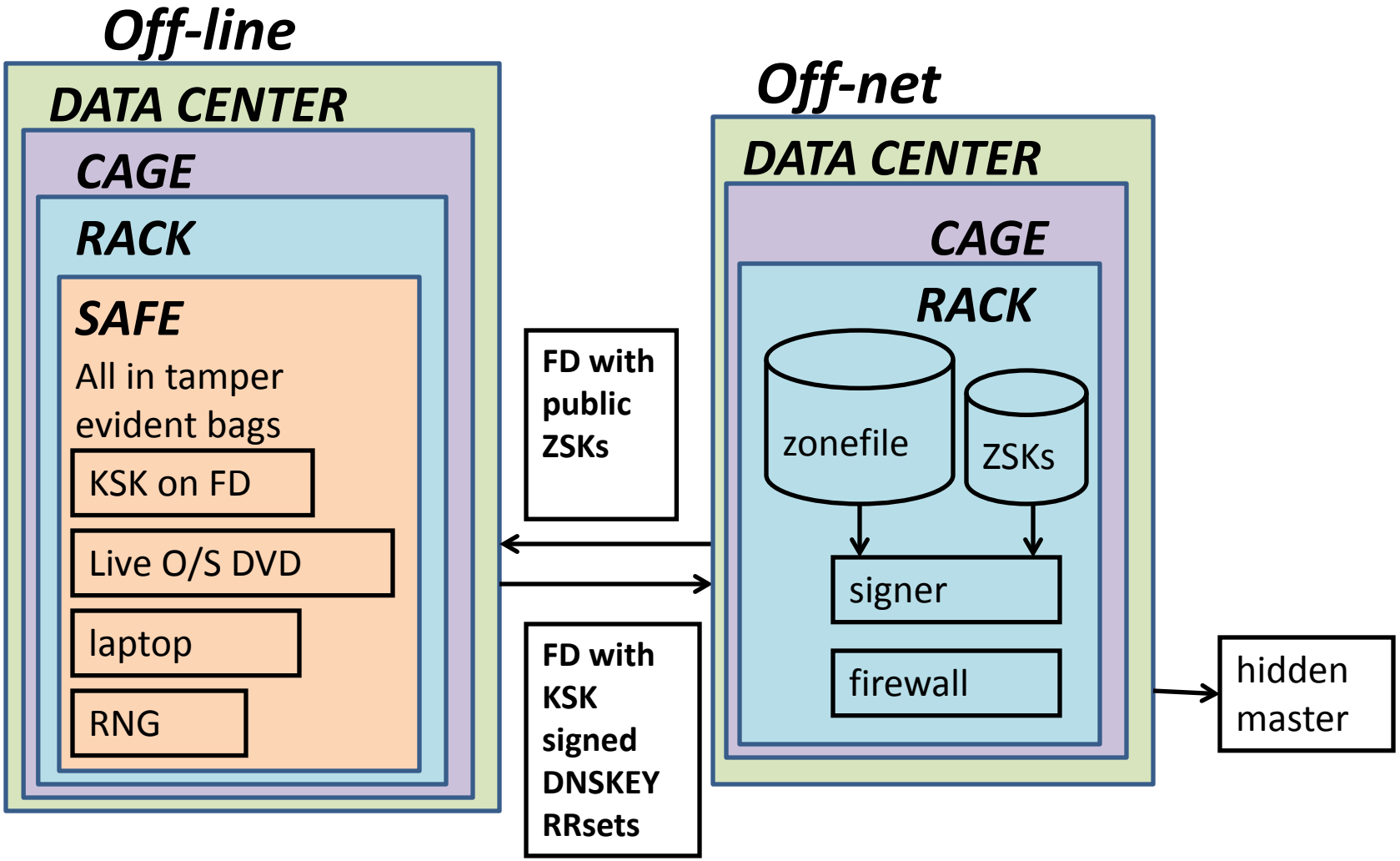
Director, Industry Program Group
Communications Security Establishment



..or this (from .cr)

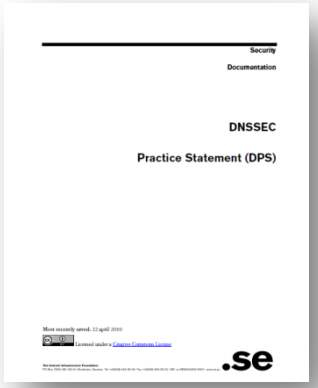


…or even this


Off-line
DATA CENTER
CAGE
RACK
SAFE
All in tamper evident bags
KSK on FD
Live O/S DVD
laptop
RNG
FD with public ZSKs
FD with KSK signed DNSKEY RRsets
Off-net
DATA CENTER
CAGE
RACK
zonefile
ZSKs
signer
firewall
hidden master

But all must have:

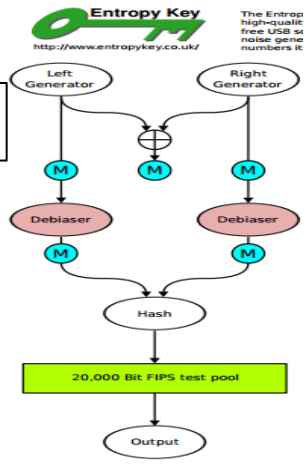
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability



- Documented procedures for each operation
- Multi person access requirements
- Audit logs
- Good Random Number Generators

15 Feb 12 – "Ron was wrong, Whit is right"

Intel RdRand



DRBGs

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Summary

- DNSSEC has left the starting gate but without greater support by Registrars, ISPs and domain name holders and trustworthy deployment it...
- Building awareness amongst a larger audience based on recent attacks and pronouncements may be the solution.
- Drawing on lessons learned from certificate authorities makes sure DNSSEC becomes a source of opportunity and innovation floating all boats

Resultant Global PKI
SSL (DANE), E-mail, VOIP security…

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

Securing VoIP

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/

+1-202-709-5262
VoIP

US-NSTIC

DNS is a part of all ecosystems

facebook

PayPal

ebay

AADHAAR

Google OpenID

OECS ID effort

amazon Prime

e-Passport symbol

PASSPORT

COUNTRY of Origin

ICP Brasil

O Brasil na era da certificação digital

DigiNotar

A VASCO COMPANY

COMODO

Creating Trust Online

Smart Electrical Grid

Trust frameworks are not new

Identity providers

Relying parties

Exchange (clearing house)

users

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Proves your identity to a remote computer

Norton SECURED

powered by VeriSign

lamb@xtcn.com