DNSSEC Implementation at .CR

ccNSO TechDay
Luis Espinoza S.
CTO – NIC Costa Rica
Agenda

• Introduction
• Planning
• Research and development
• Implementation
• The results.
Introduction

• Evil things come up to DNS:
  – Man in the middle attacks (cache poisoning).
  – Virus (Conficker).
  – Provide: Identity theft (phishing)
  – Results: Bank fraud or worst!
Introduction

Security

Stability

DNSSEC

Awnccast

OWASP

Reliability

Availability

Performance
Implementation

- Focus on Financial .fi.cr
- Create trust
- Complete the chain
Implementation details

• Look for an important Bank under .fi.cr to present a pilot project – Banco Nacional de Costa Rica.
• Implement DNSSEC for .fi.cr and chain with .cr, then chain with root-servers.
• Use hardware based solution (new low cost solution based on TPM).
• DNSSEC Policy Statement
Goals Achieved

- Banco Nacional embrace DNSSEC
- Signer using TPM
- Signing and re-signing integrated within work flow
- DPS in Spanish
Secondary Name Servers distribution for .cr

- Basic Coverage: May 2011 - Mexico, USA, RIPE (EU), C.R.
- New coverage: Chile
- New coverage - Anycast: East Coast, West Coast, Asia, Europe.

www.nic.cr  /  correo@nic.cr  /  Teléfono: (506) 2280-6453 / Fax: (506) 2280-5261
Verify Signed Zone

BIND&DNS

EPP

ns.cr (UCR) MASTER

ns.cr (NIC) MASTER

ISC Anycast

RIPE Anycast

CHILE

MX

Publíc

Privado

www.nic.cr

Fred - Client

DNSSEC Signer

Gen-zone

Verify zone

Verify Signed Zone

Reload+Notify

Oculto

secundario.nic.cr

NIC-CR+DNSSEC
Main issues

- Cisco firewall:
  - policy-map type inspect dns preset_dns_map
  - Parameters
  - message-length maximum 4096.

- Find how to backup TPM keys before place sign in production environment.

- Process to approve and publish DPS.
bnonline.fi.cr

• Face to face meeting to awareness about the benefits of DNSSEC.
• Technical work session to explain concepts.
• Self signing process and email send of the DS.
• Incorporation of DS of bnonline.fi.cr within db..fi.cr via hourly script (don’t use Fred for this yet).
Checking with dnsviz.net
DNSSEC Verification
Key management room

- Security Camera
- Offline PC with TPM
Key backup and custody

Tamper evidence bags labeled

3 USB flashdrives with copies of Keys. Local and remote (bank) in safeboxes
Thanks!

lespinoz@nic.cr