

DNSSEC: Securing the Domain Name System

“Why and how”

AfTLD/ISOC meeting

mauritius, 30th November 2006

Alain AINA Patrick

aalain@afnic.net

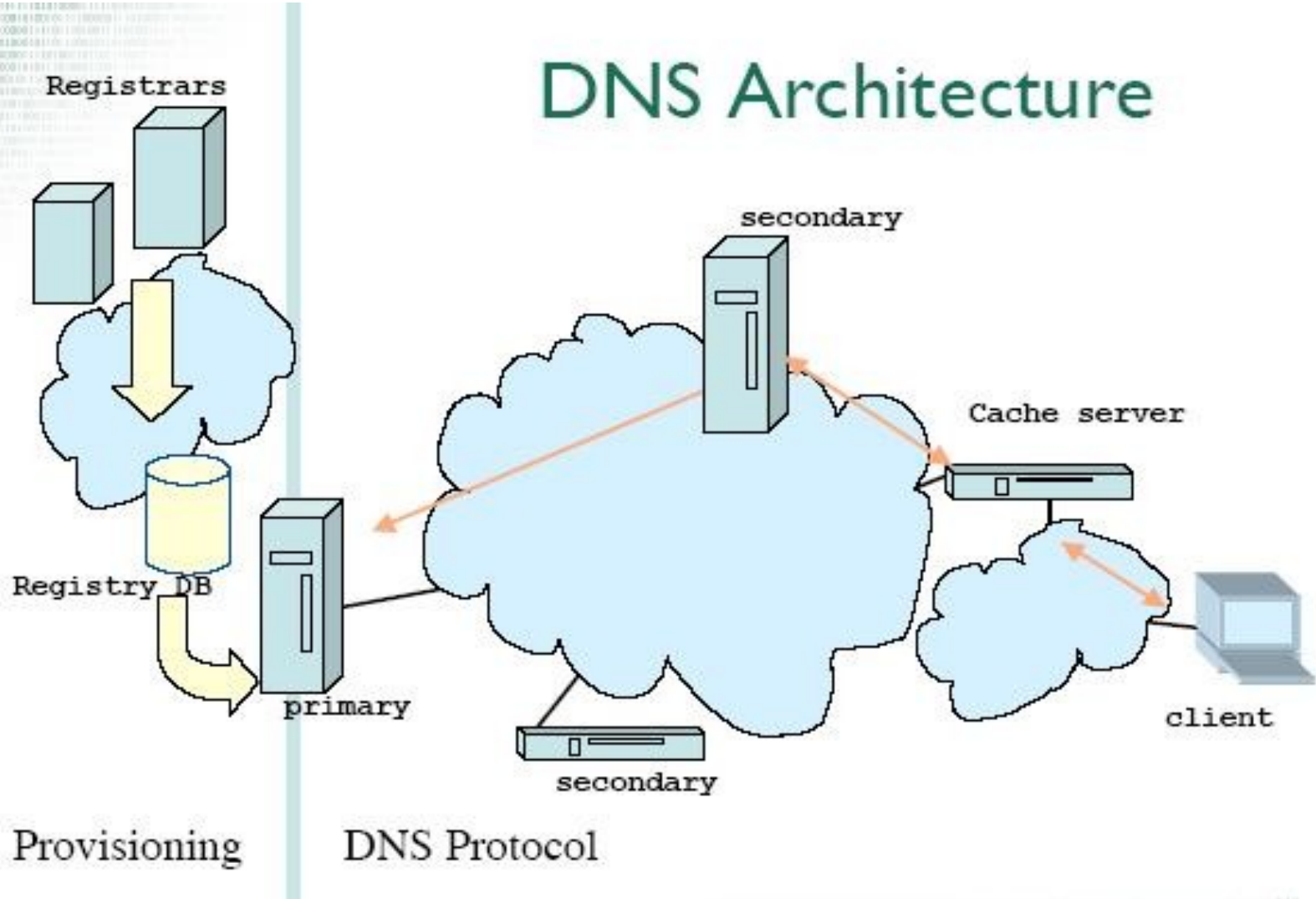
Why DNSSEC

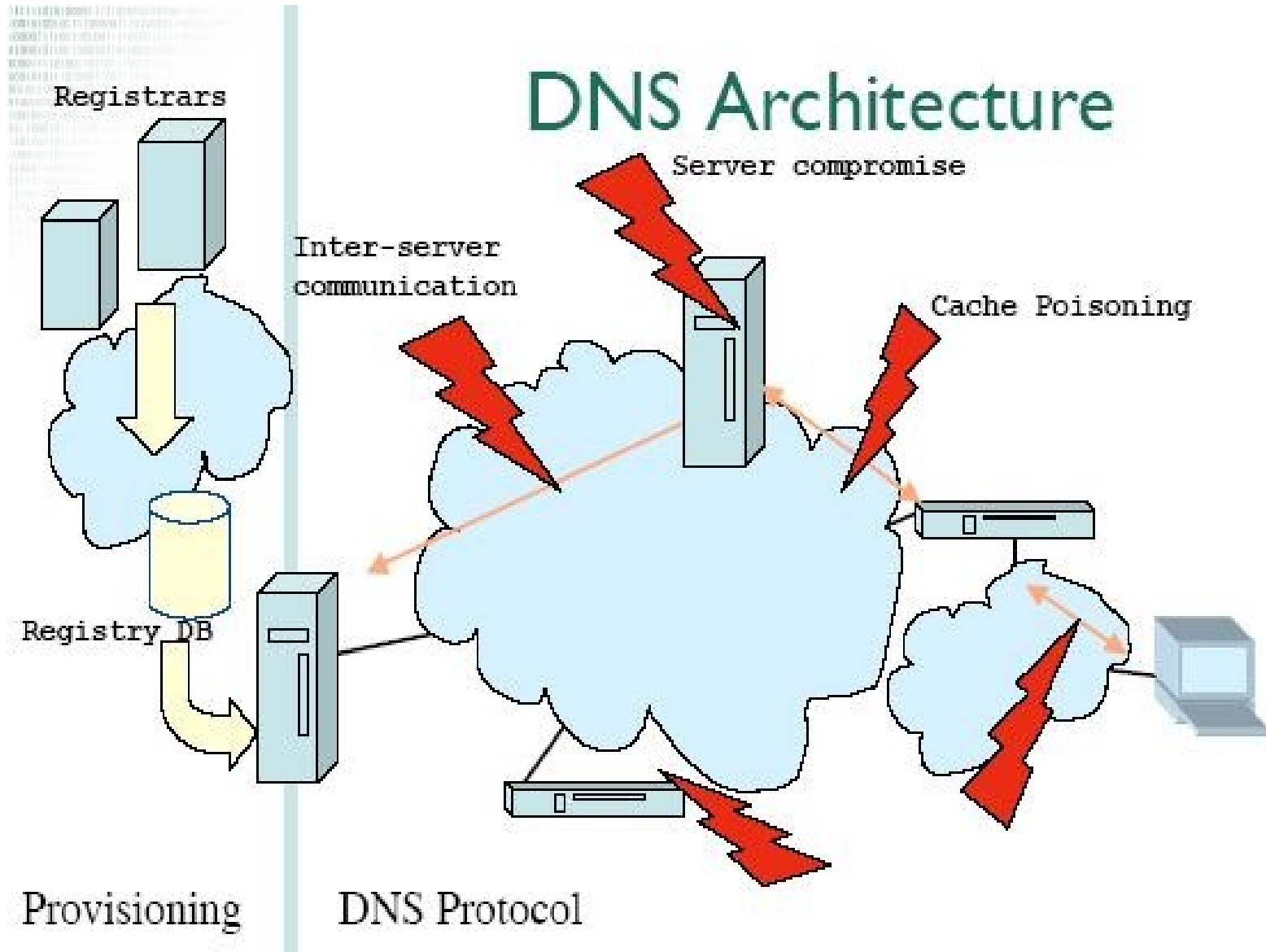
- Good security is multi-leveled
 - Multiple defence rings in physical secured systems
 - Multiple 'layers' in the networking world
- DNS infrastructure
 - Providing DNSSEC to raise the barrier for DNS based attacks
 - Provides a security 'ring' around many systems and applications

The Problem

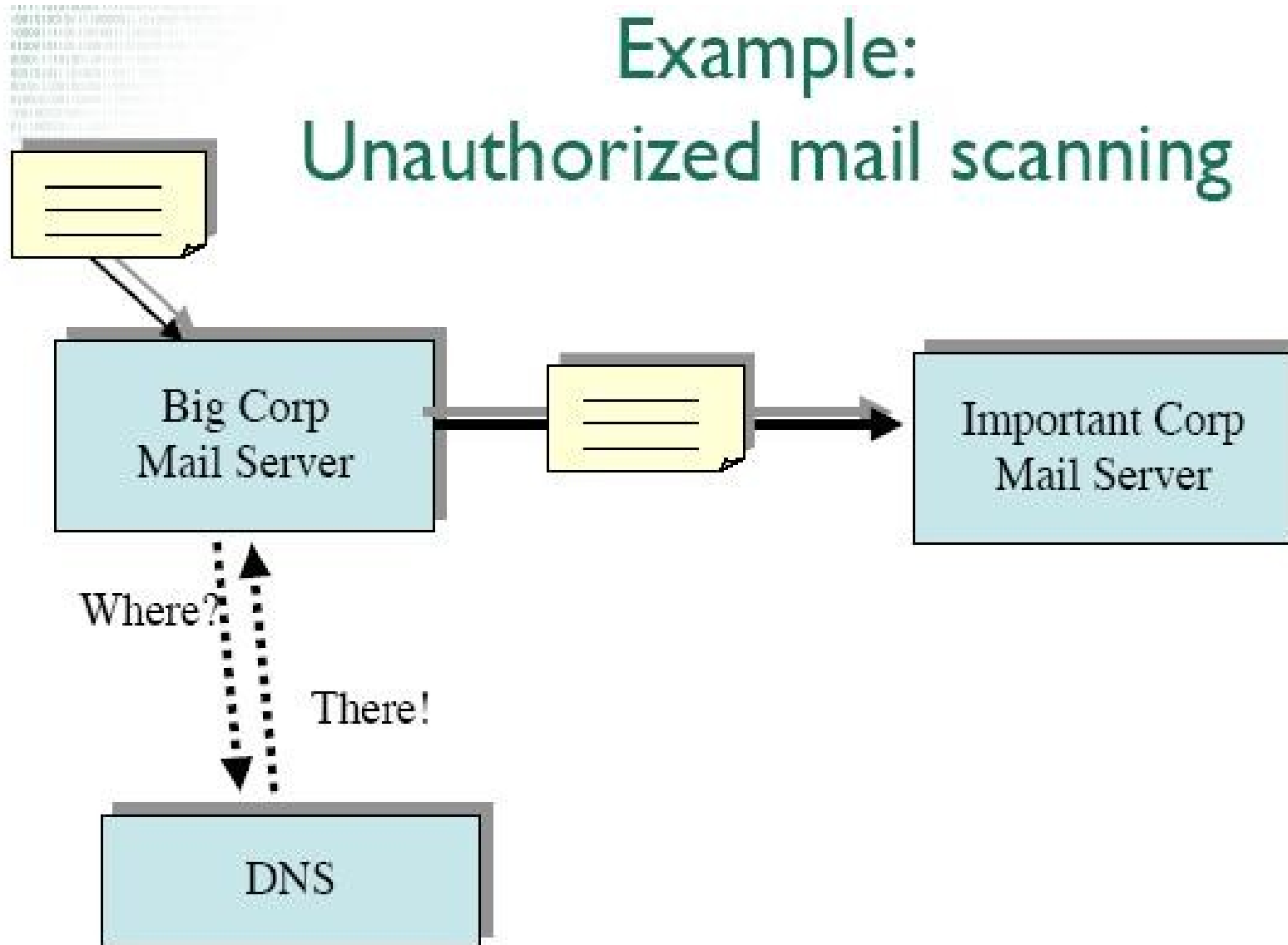
- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
 - Some places are more vulnerable to attacks than others
 - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)

DNS Architecture

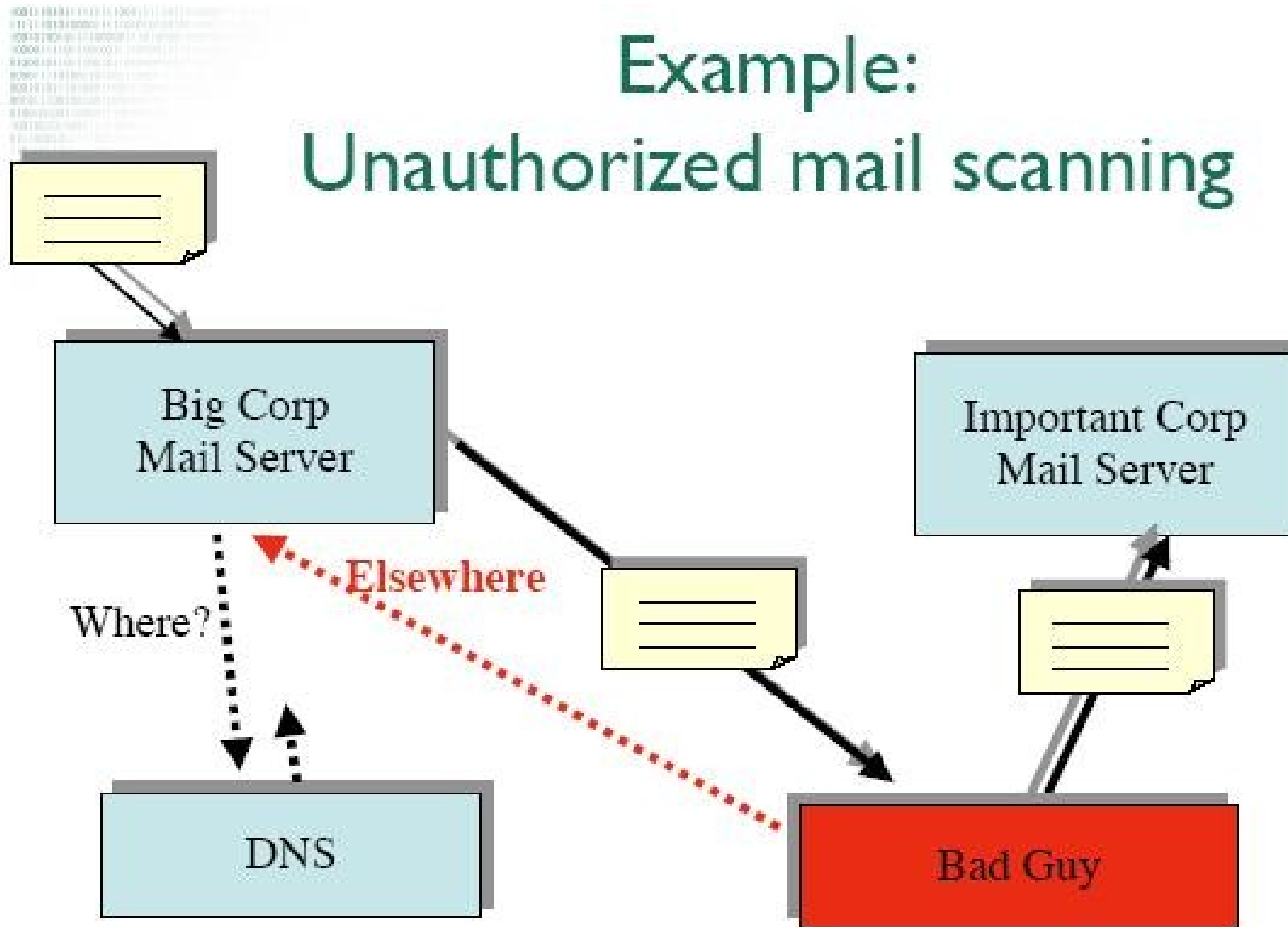




Example: Unauthorized mail scanning



Example: Unauthorized mail scanning



Targets...

Where do DNS and economics meet?

- SPF, DomainKey and family
 - Technologies that use the DNS to mitigate spam and phishing: \$\$\$ value for the black hats
- Stock tickers, RSS feeds
 - Usually no source authentication but supplying false stock information via a stock ticker and via a news feed can have \$\$\$ value
- ENUM
 - Mapping telephone numbers to services in the DNS

DNSSEC Properties

- DNSSEC provides message authentication and integrity verification through cryptographic signatures
 - Authentic DNS source
 - No modifications between signing and validation
- It does not provide authorization
- It does not provide confidentiality

(...)

trstech.net. 86400 NS ns.trstech.net.

trstech.net. 86400 NS rip.psg.com.

trstech.net. 86400 **RRSIG** NS 5 2 86400 20061227191027 (20061127191027 33888

trstech.net.pVlziETr5b3RjBR86rHTdgrJVEkL9QfHoUoR3mepL5wGIH8leJpeZQNjQPZM/AMzcEtiDmli2RXvpYLxTdBpd
g==)

(....)

trstech.net. 86400 **DNSKEY** 257 3 5

(AwEAAZrwNevGbMaT+yW9K+XILk6WqN3F1heks/tfUCjAVWLKYHKtB5+2GdCC7QW4MA3dwAKbpqv+4NSg/6yL
wQzBnF6gSRW3PhzIR53u8FdGF3yuYzTOd8HSL04otkZfmXAWnDSJfLY0WkZyycxB+tMWUWqEYWMhC5aZuTL7kHJn
diz3) ; key id = 36472

(.....)

trstech.net. 86400 **RRSIG** DNSKEY 5 2 86400 20061227191027 (20061127191027 33888 trstech.net.

J82iBTIEZOoheOMigH52SLtHtXHij9JT12RlepZr9+EAeW/24wjJqvkcWLRN1DFYXTbK1V24F9NzkUh5TfeFw==)

(...)

trstech.net. 3600 **NSEC** aalain.trstech.net. NS SOA MX RRSIG NSEC DNSKEY

trstech.net. 3600 **RRSIG** NSEC 5 2 3600 20061227191027 (20061127191027 33888 trstech.net.

TE9+FGO2Yr5fwOu3/uXyW/Ub4M6YobJNkhhTWW835Ff2qmZrpraFLp5ZNAK200M901uY7XI20O8nvRDv8XXb9Q==)

(...)

DNSSEC Deployment Tasks

- Key maintenance policies and tools
 - Private key use and protection
 - Public key distribution
- Zone signing and integration into the provisioning chain
- DNS server infrastructure
- Secure delegation registry changes
 - Interfacing with customers

Key maintenance

- DNSSEC is based on public key cryptography
 - Data is signed using a private key
 - It is validated using a public key

Operational problems:

- Dissemination of the public key
- Private key has a 'best before' date
 - Keys change, and the change has to disseminate

Public key Dissemination

- In theory only one trust-anchor needed that of the root
 - How does the root key get to the end user?
 - How is it rolled?
- In absence of hierarchy there will be many trust-anchors
 - How do these get to the end-users?
 - How are these rolled?
- These are open questions, making early deployment difficult

Typical Public Key Dissemination

In absence of a signed parent zone and automatic rollover:

- Trust anchors are published on an “HTTPS” secured Website
- Trust anchors are signed with the owner's public keys
- Trust anchor can be rolled twice a year (during early deployment)
- Announcements and publications are always signed by x.509 or PGP

Key Management

- There are many keys to maintain
 - Keys are used on a per zone basis
 - o Key Signing Keys and Zone Signing Keys
 - During key rollovers there are multiple keys
 - o In order to maintain consistency with cached DNS data[rfc 4641]
- Private keys need shielding

Infrastructure

- One needs primary and secondary servers to be DNSSEC protocol aware
- We had a number of concerns about memory CPU and network load
 - Research done and published as RIPE 352

Providing secure delegations

- The DS (Delegation Signer) exchange is the same process as the NS exchange
 - Same authentication/authorization model
 - Same vulnerabilities
 - More sensitive to mistakes
- Integrate the key exchange into existing interfaces
 - Customers are used to them
- Include checks on configuration errors
 - DNSSEC is picky
- Provide tools
 - To prevent errors and guide customers

readings

- <http://www.dnssec.net>
- Rfcs 4033,4034,4035
- Rfc 4641

Thank you for your attention

Questions ?