

# DNS FORUM BENIN 2015

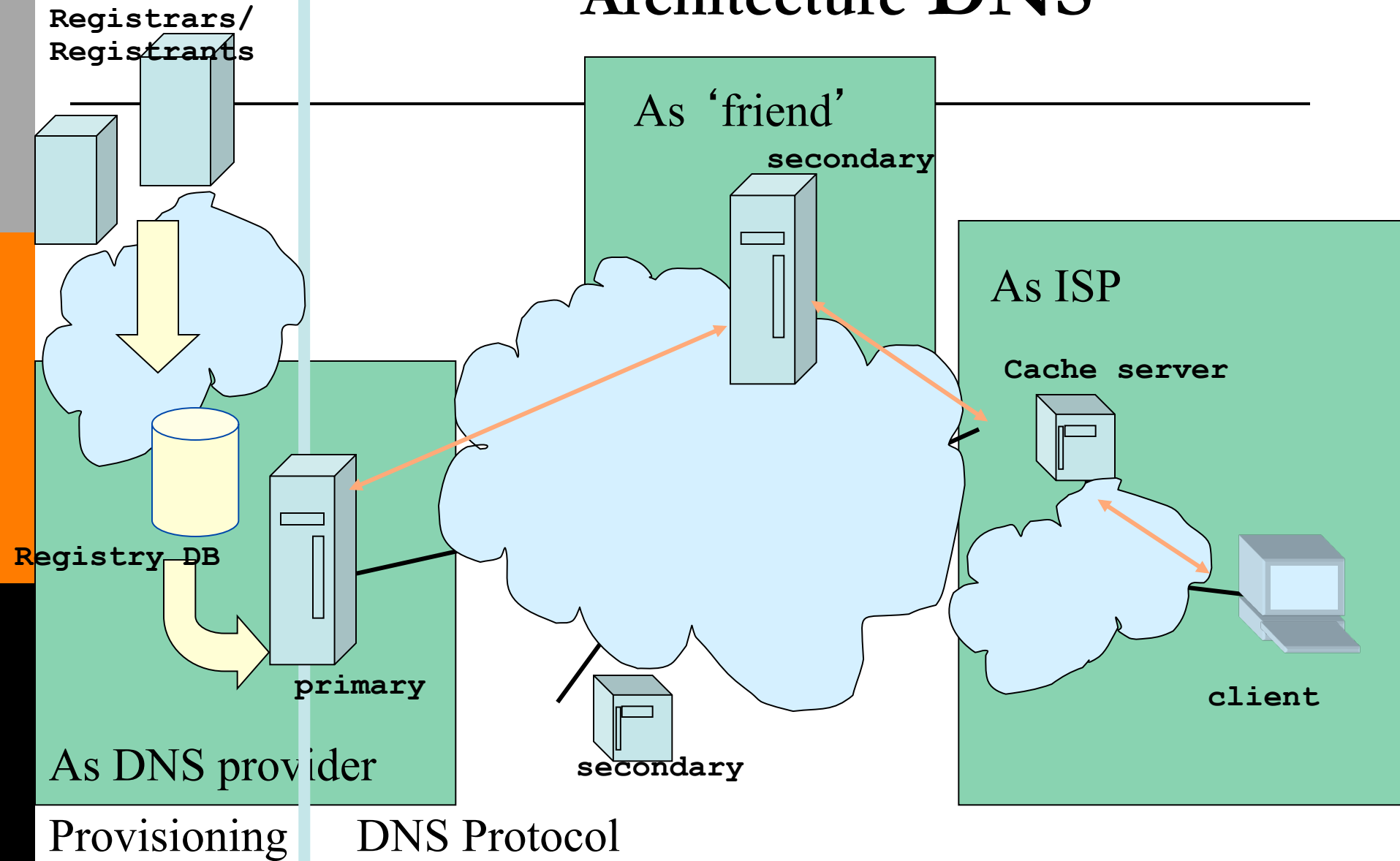
---

## RESILIENCE ET SECURITE DNS

Alain Patrick AINA  
Root KSK Crypto Officer  
[aalain@trstech.net](mailto:aalain@trstech.net)

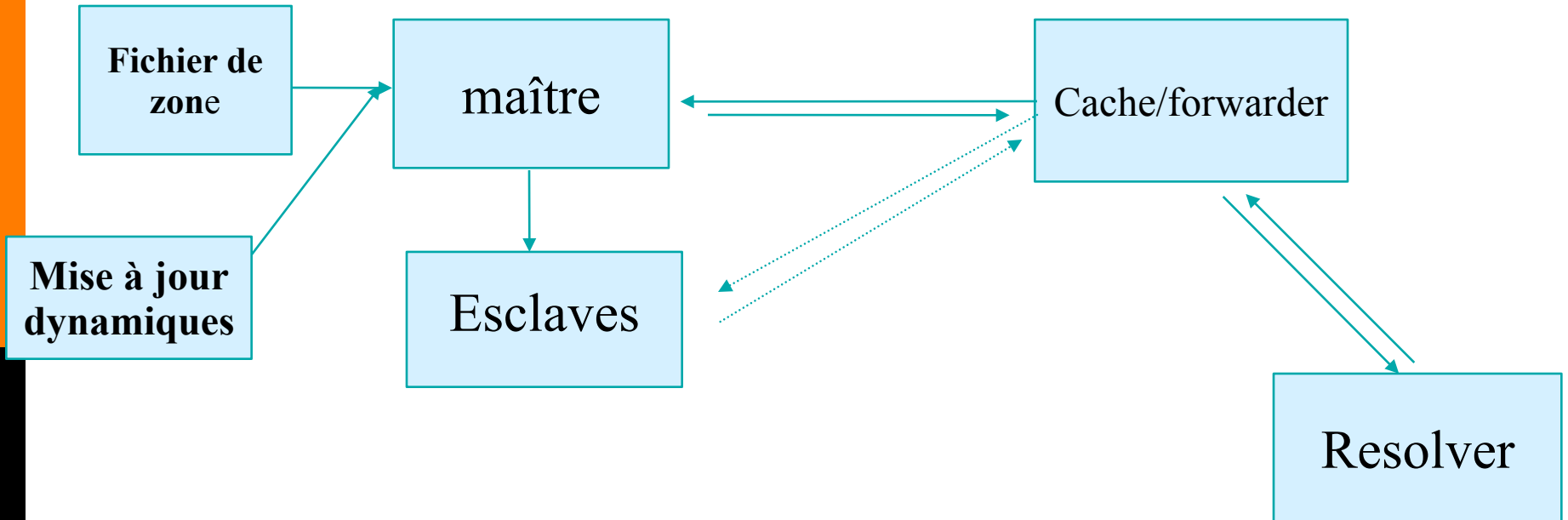
12/12/15

# Architecture DNS



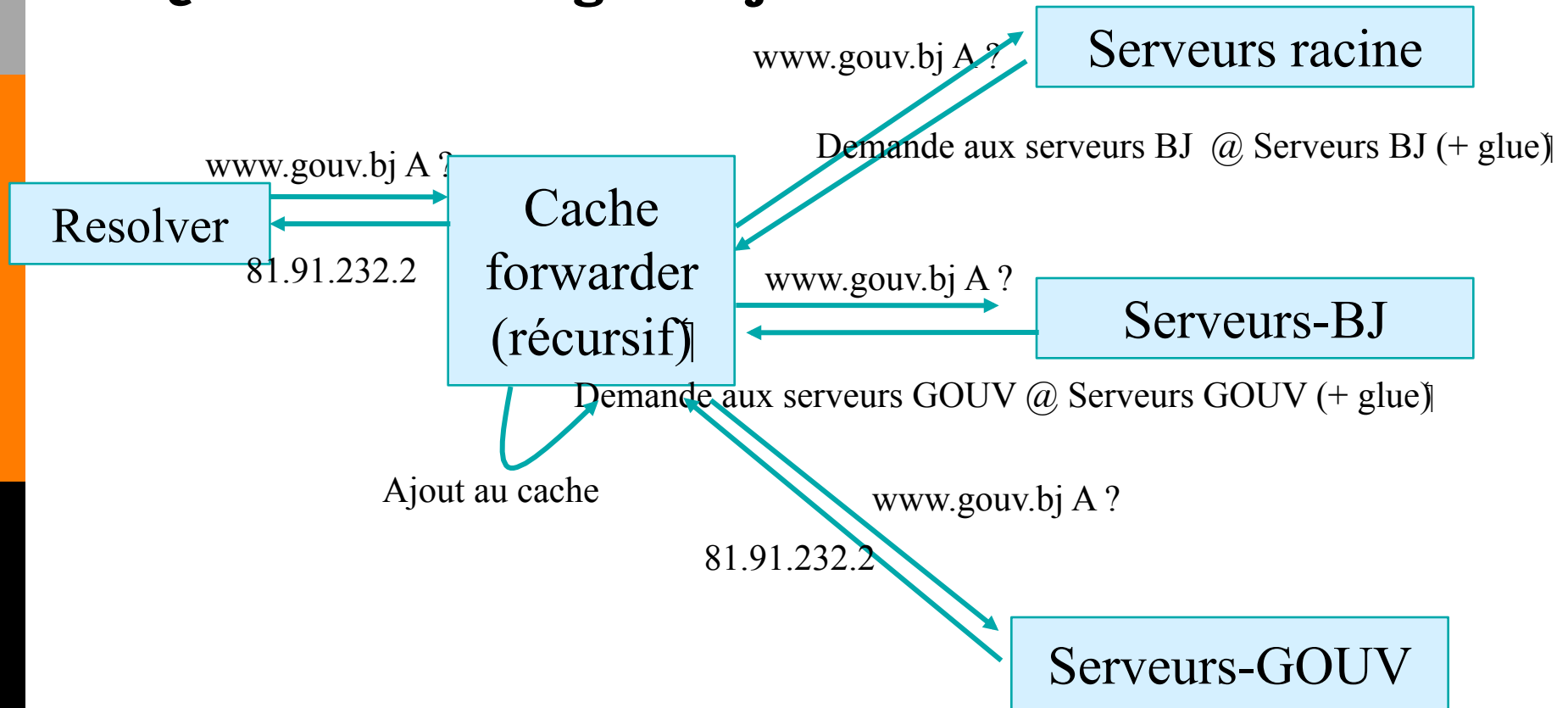
# Mouvement des données DNS

---

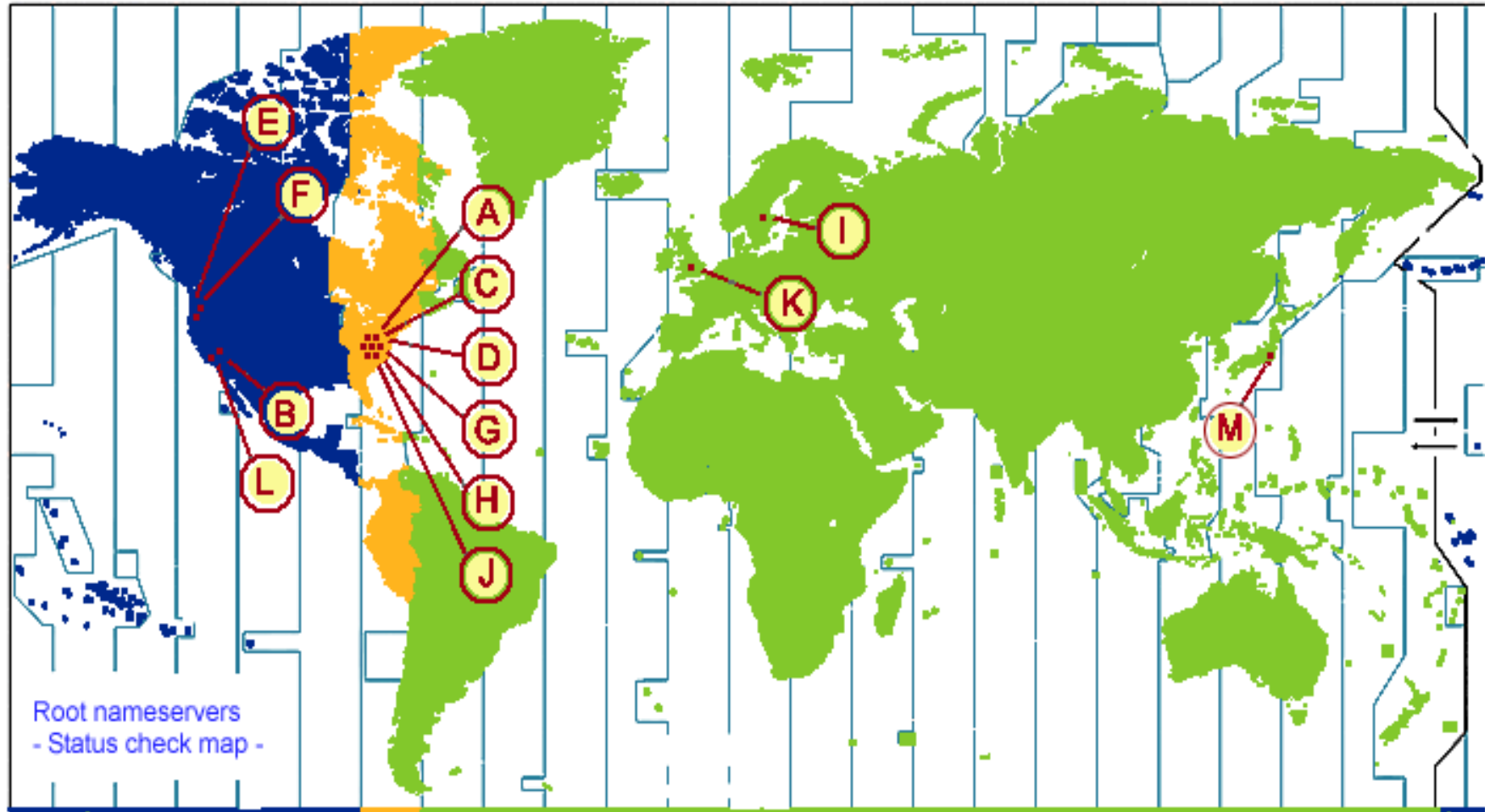


# Résolution DNS

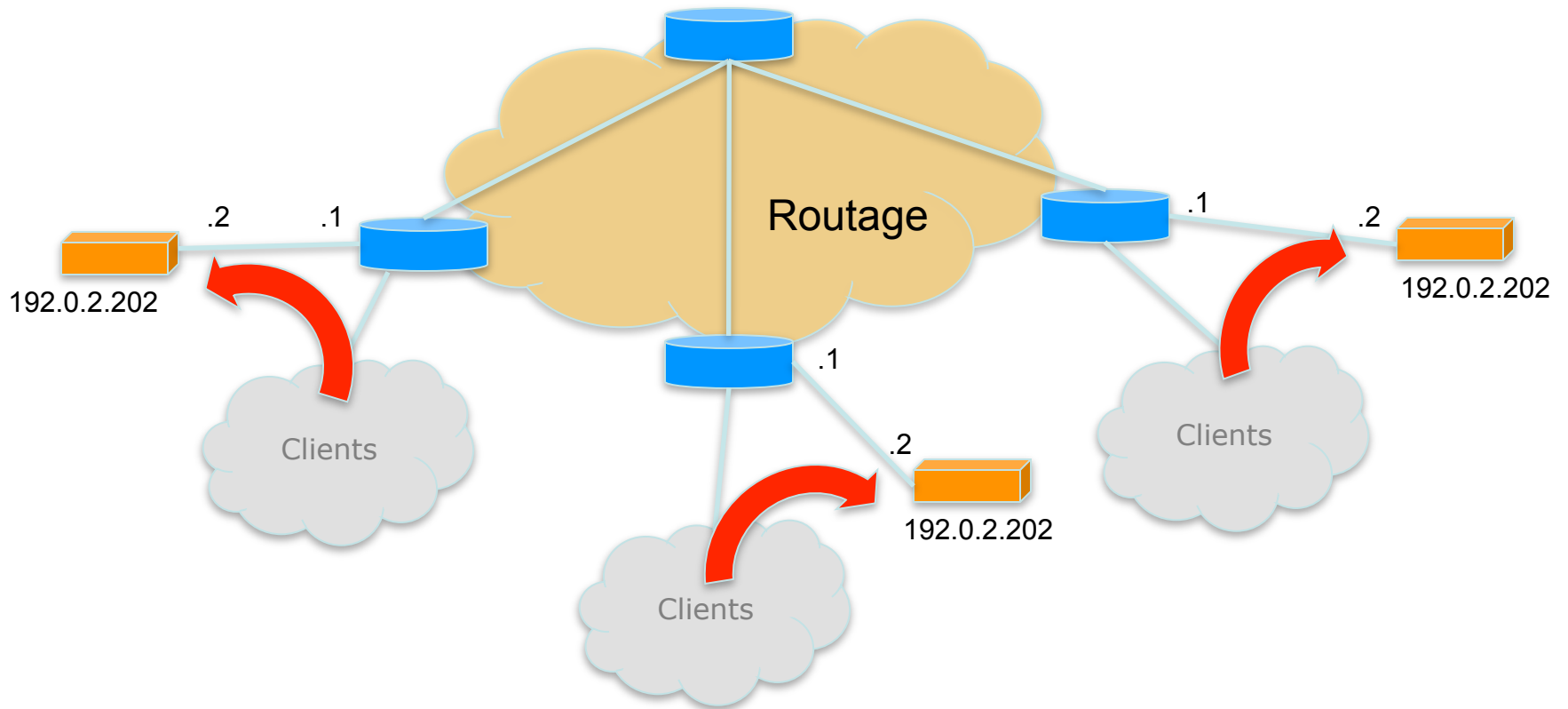
**Question: www.gouv.bj A**



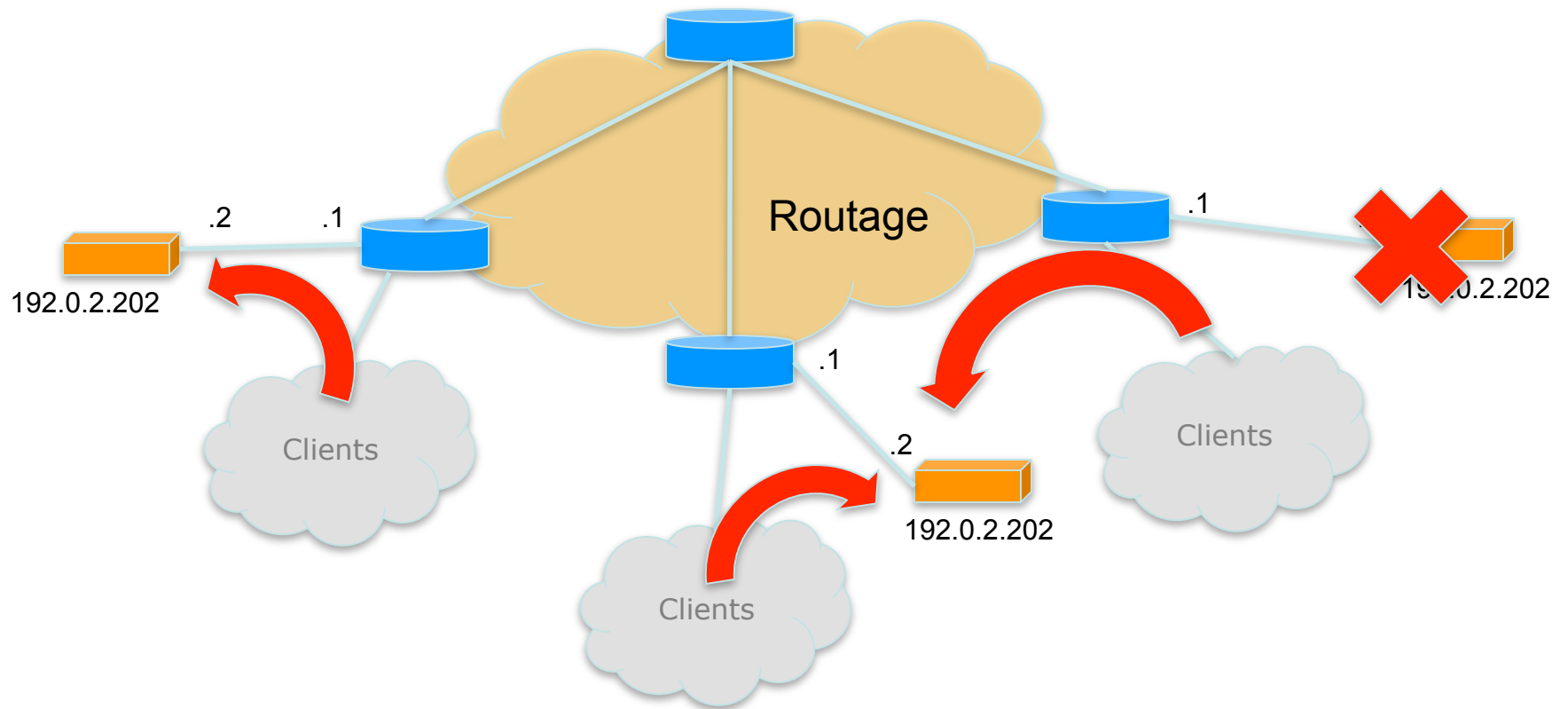
# Opérateurs Serveurs Racine



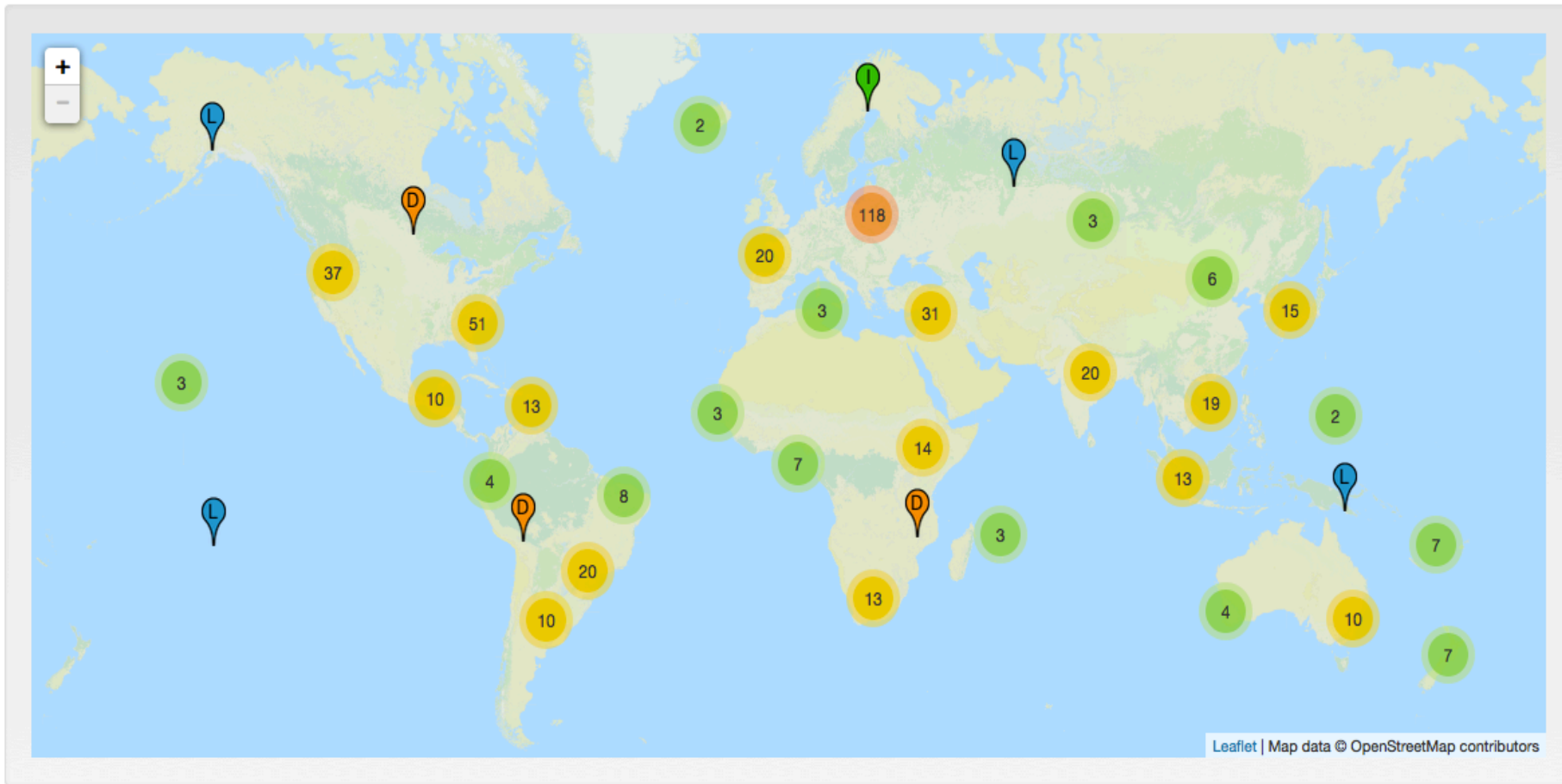
# Topologie Anycast



# Topologie Anycast

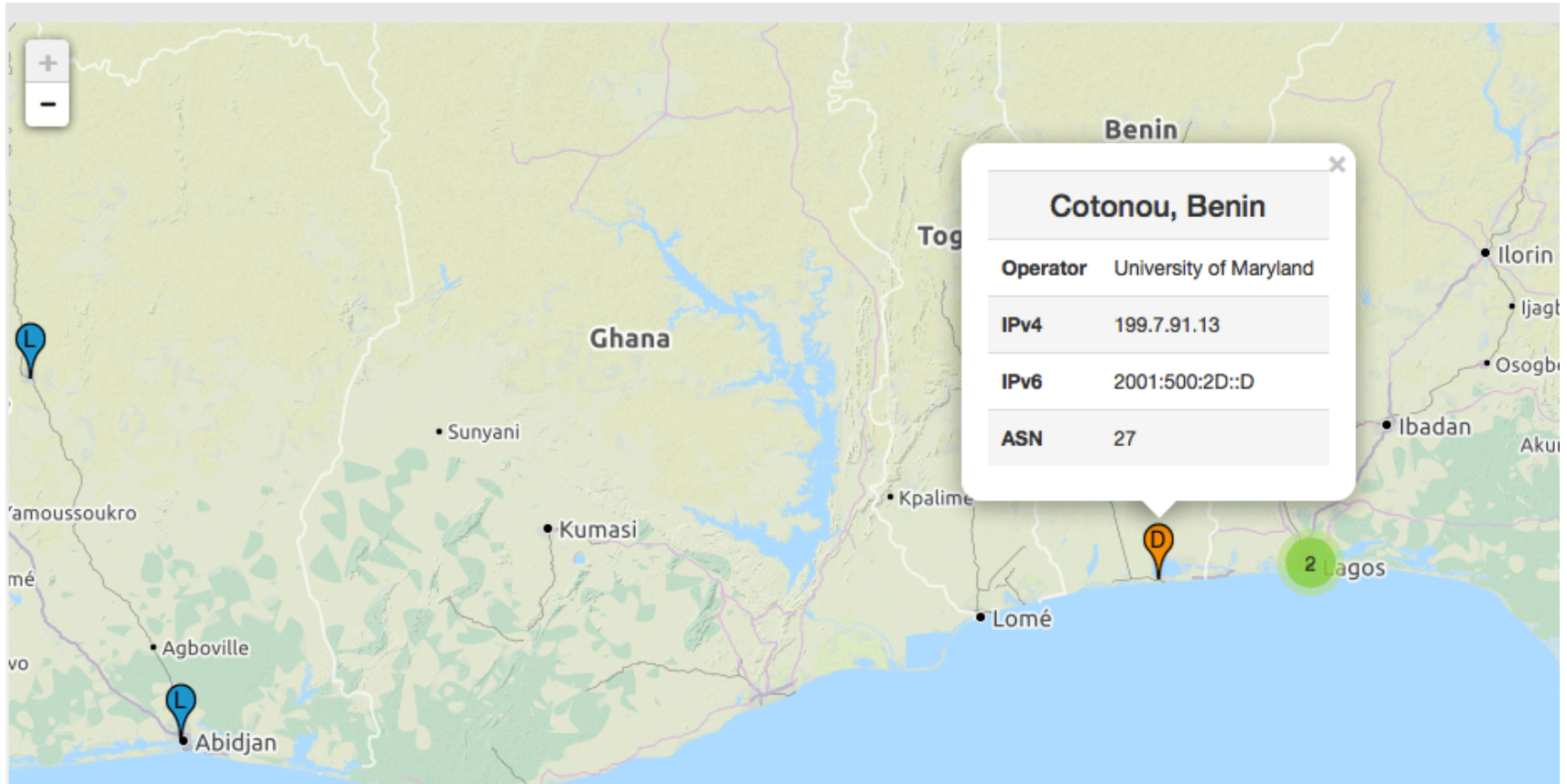


# Distribution Serveurs Racine via Anycast



[www.root-servers.org](http://www.root-servers.org)

# Distribution Serveurs Racine via Anycast



D-root @Cotonou

# Pourquoi DNSSEC

---

- ❑ Une bonne sécurité est multicouche
  - De multiples cycles de défenses physiques des systèmes sécurisés
  - Couches multiples dans le monde de gestion des réseaux
- ❑ Infrastructure DNS
  - DNSSEC pour constituer une barrière contre les attaques basées sur le DNS.
  - Fournit un anneau de sécurité autour de plusieurs systèmes et applications

# Le Problème

---

- Les données DNS publiées sont remplacées en transit entre serveurs et clients.
- Ceci peut se produire à plusieurs endroits dans l'architecture DNS
  - **DNS utilise UDP, beaucoup plus facile à falsifier**
  - **Certains endroits sont plus vulnérables que d'autres**
  - **Les vulnérabilités dans les logiciels DNS facilitent les attaques**  
**(et il y aura toujours de vulnérabilités de logiciel)**
- Carences dans le protocole DNS et dans les déploiements classiques créent quelques faiblesses.
  - **Le Query ID est de 16 bits (0-65535)**
  - **Manque de randomisation de port source (16 bits) et de Query ID de paquets UDP dans certains déploiements.**

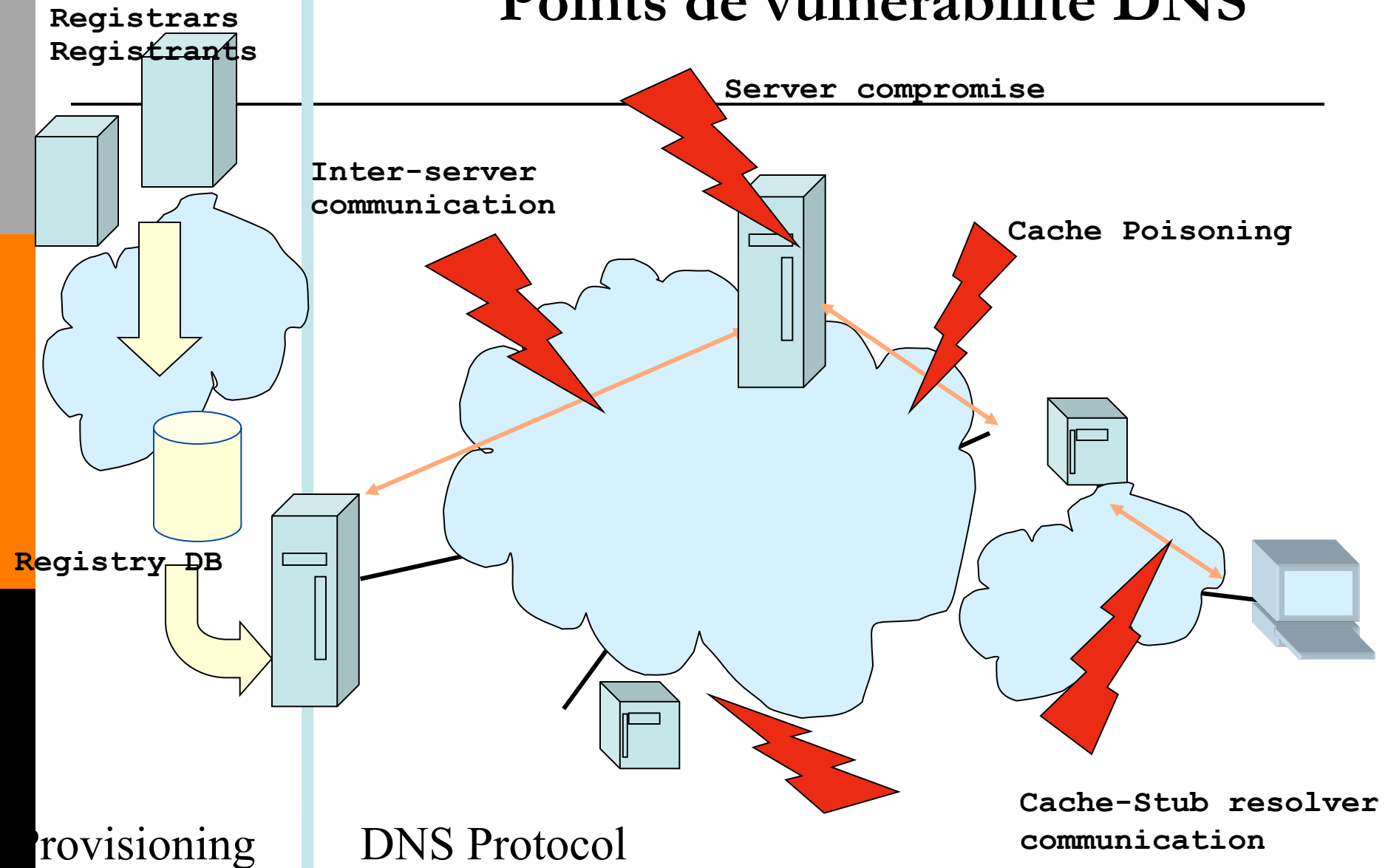
# Le Problème (suite)

---

- Les attaques de Kaminsky publiées en 07/2008 ont montré comment ces faiblesses peuvent être exploitées pour des attaques de pollution de cache
  - Panique (bien que tout cela soit connu depuis!!! )
  - Contournements pour contenir la situation
    - **Randomisation de port source/Query ID**
    - **Recommandations pour le déploiement DNS**  
<http://www.kb.cert.org/vuls/id/800113>
  - La Solution ????
    - **DNSSEC**

**Et ainsi, DNSSEC est désormais connu comme un élément critique de la sécurité du DNS.**

# Points de vulnérabilité DNS



# Exemple:

## Scan de mail non autorisé

Subject: Hi

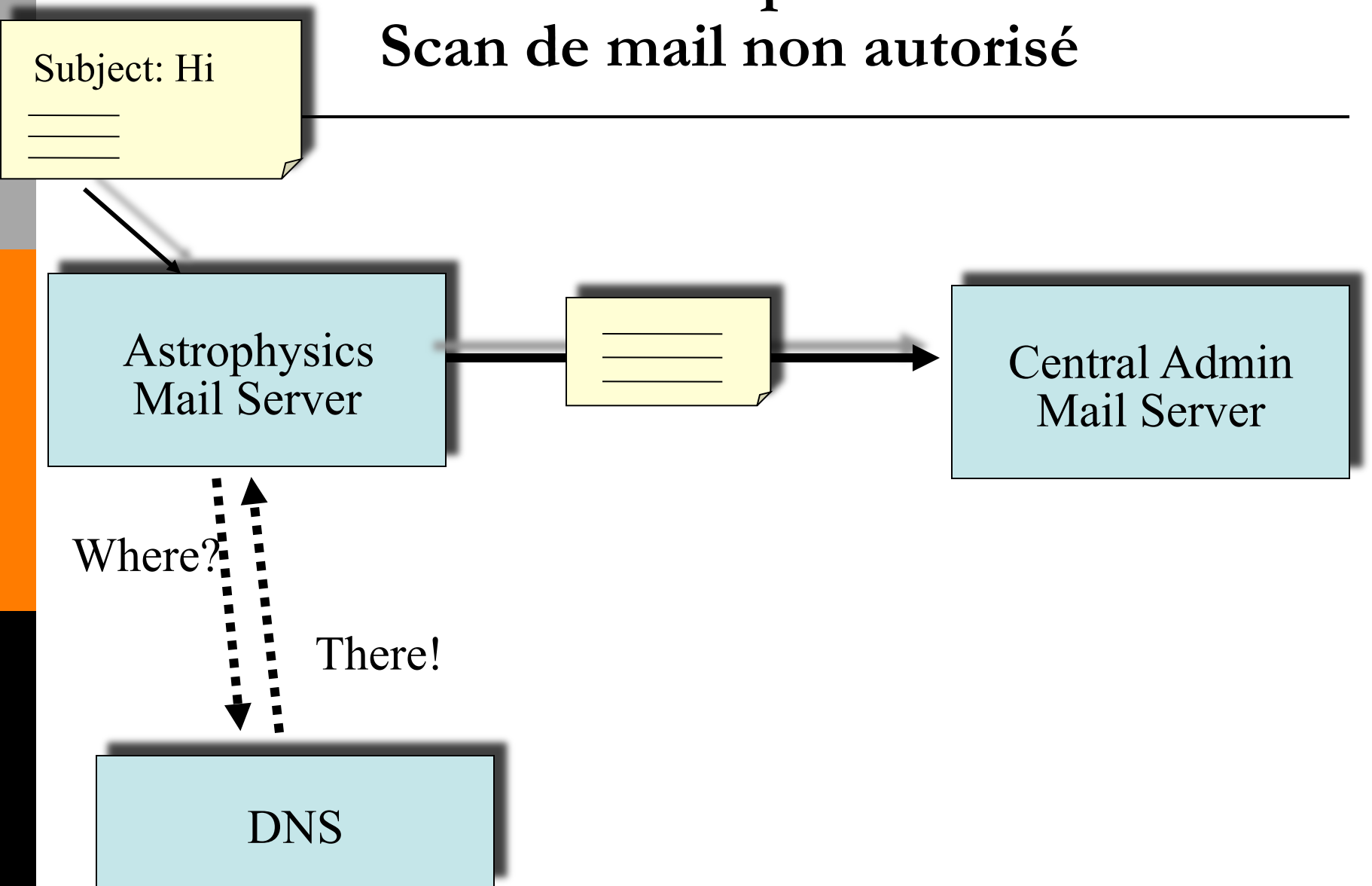
Astrophysics  
Mail Server

Central Admin  
Mail Server

Where?

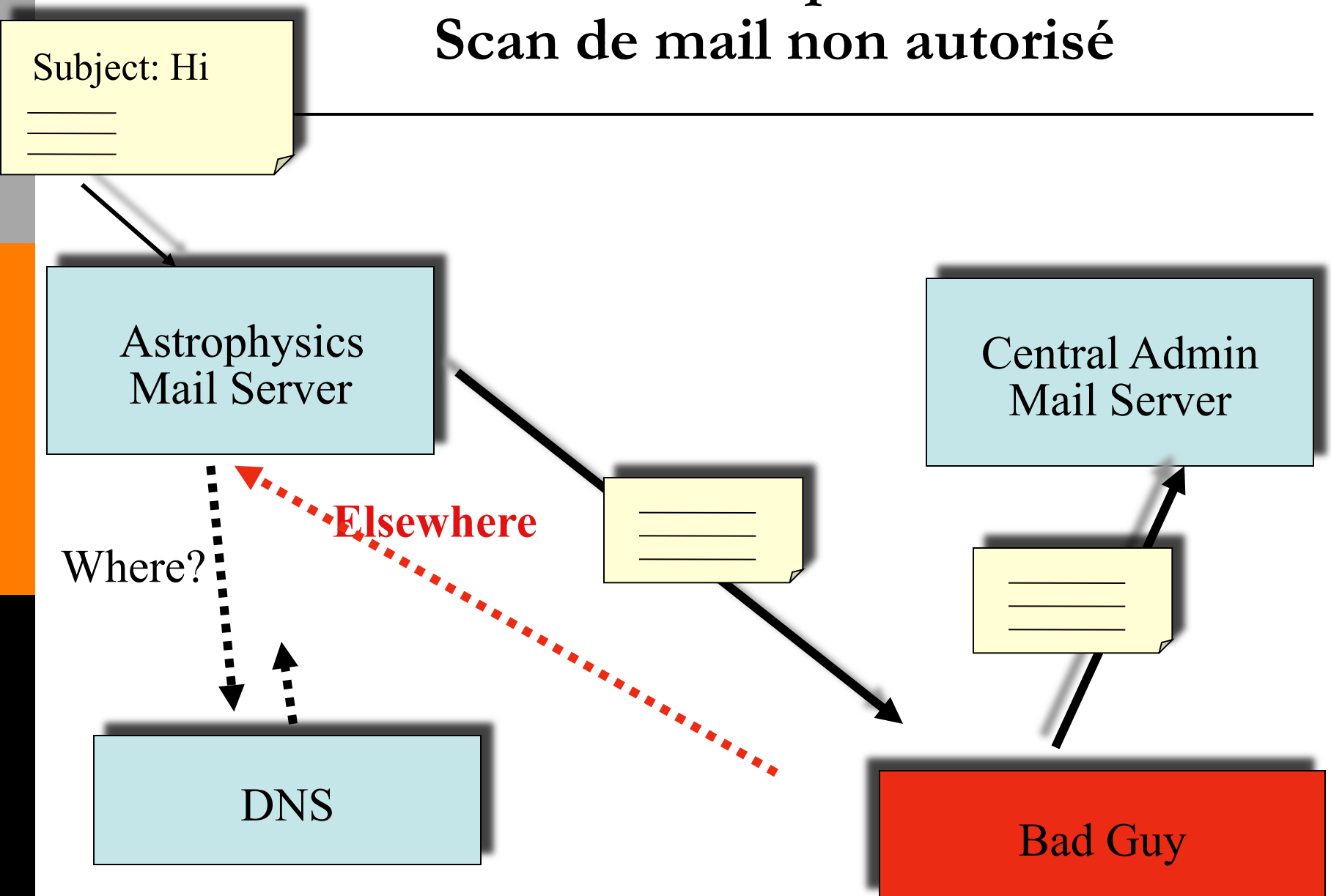
There!

DNS

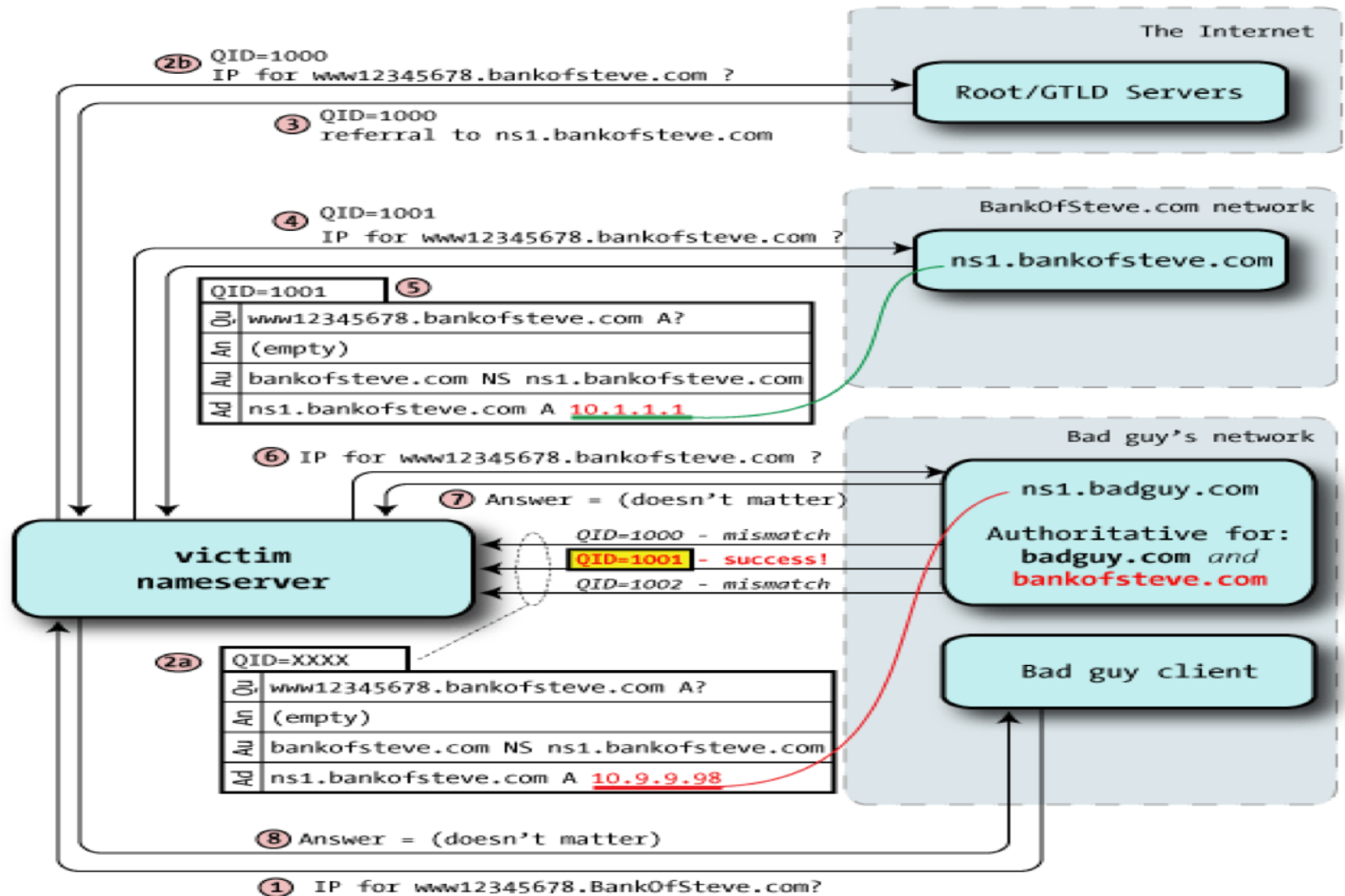


# Exemple:


## Scan de mail non autorisé



# Attaques de Kaminsky



# Attaques de Kaminsky (suite)

 metasploit®

Stay Updated | [Metasploit Blog](#) | [Website Feedback](#)

Search

[Home](#) [ABOUT](#) [HELP](#) [NEWS](#) [DEVELOPMENT](#) [EXPLOITS](#) [WEAR SWAG](#) [DOWNLOAD](#) [READ THE FORUMS](#)

[Home](#) > [Exploit DB](#)

## DNS BailiWicked Domain Attack

This exploit attacks a fairly ubiquitous flaw in DNS implementations which Dan Kaminsky found and disclosed ~Jul 2008. This exploit replaces the target domains nameserver entries in a vulnerable DNS cache server. This attack works by sending random hostname queries to the target DNS server coupled with spoofed replies to those queries from the authoritative nameservers for that domain. Eventually, a guessed ID will match, the spoofed packet will get accepted, and the nameserver entries for the target domain will be replaced by the server specified in the NEWDNS option of this exploit.

SEARCH OTHER MODULES >

Rank

Normal

Authors

`l)ruid < druid [at] caughtq.org >`  
`hdm < hdm [at] metasploit.com >`  
`Cedric Blancher < sid [at] rstack.org >`

Vulnerability References

[CVE-2008-1447](#)  
[OSVDB-46776](#)  
[US-CERT-VU-800113](#)  
<http://www.caughq.org/exploits/CAU-EX-2008-0003.txt>

GET METASPLOIT FOR  
**PENETRATION TESTING**  
[FREE DOWNLOAD](#)

# Où intervient DNSSEC?

---

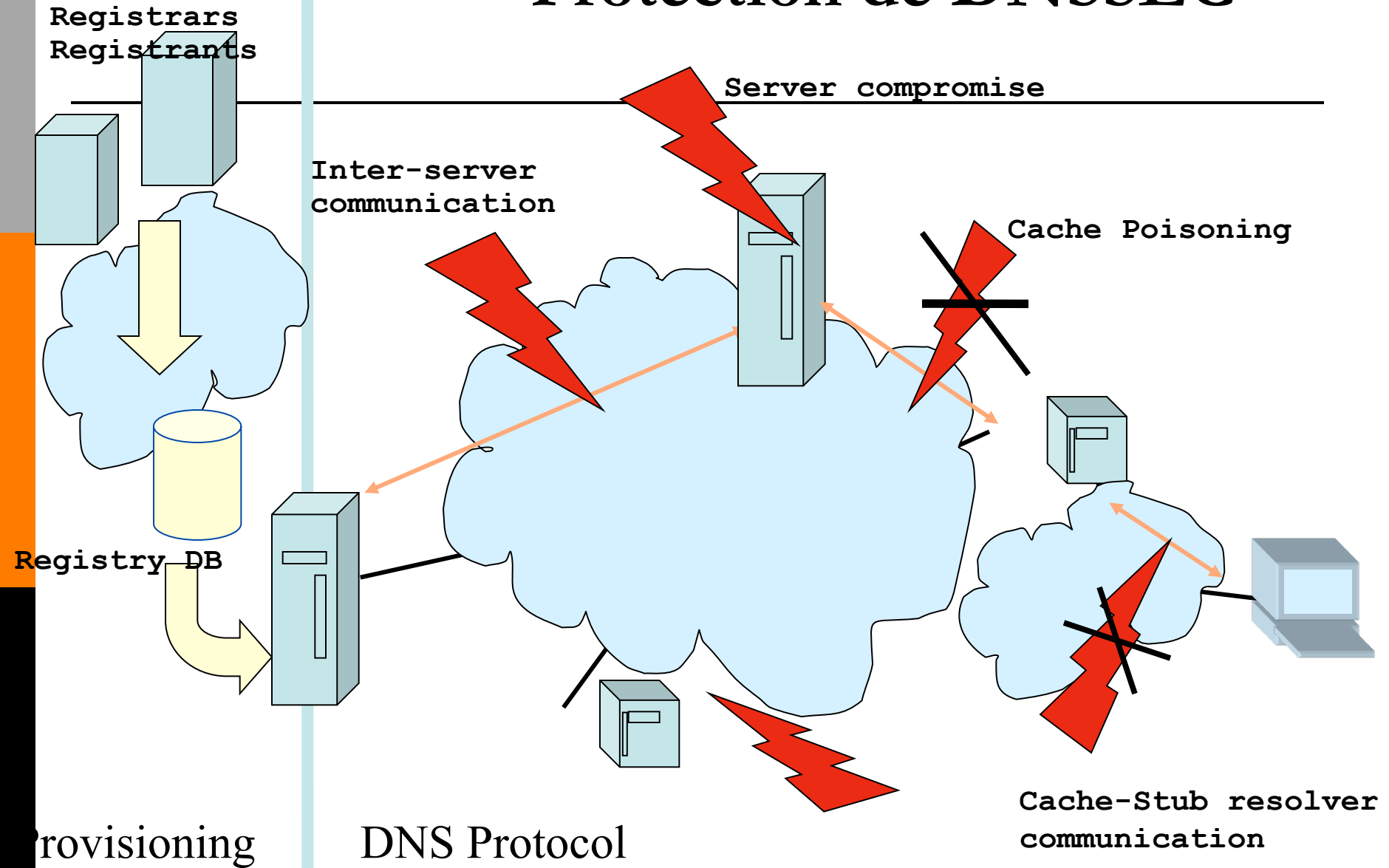
- DNSSEC sécurise le mappage des noms en adresses IP, etc...
  - La sécurité au niveau transport et applicatif est du ressort d'autres couches.

# Propriétés de DNSSEC

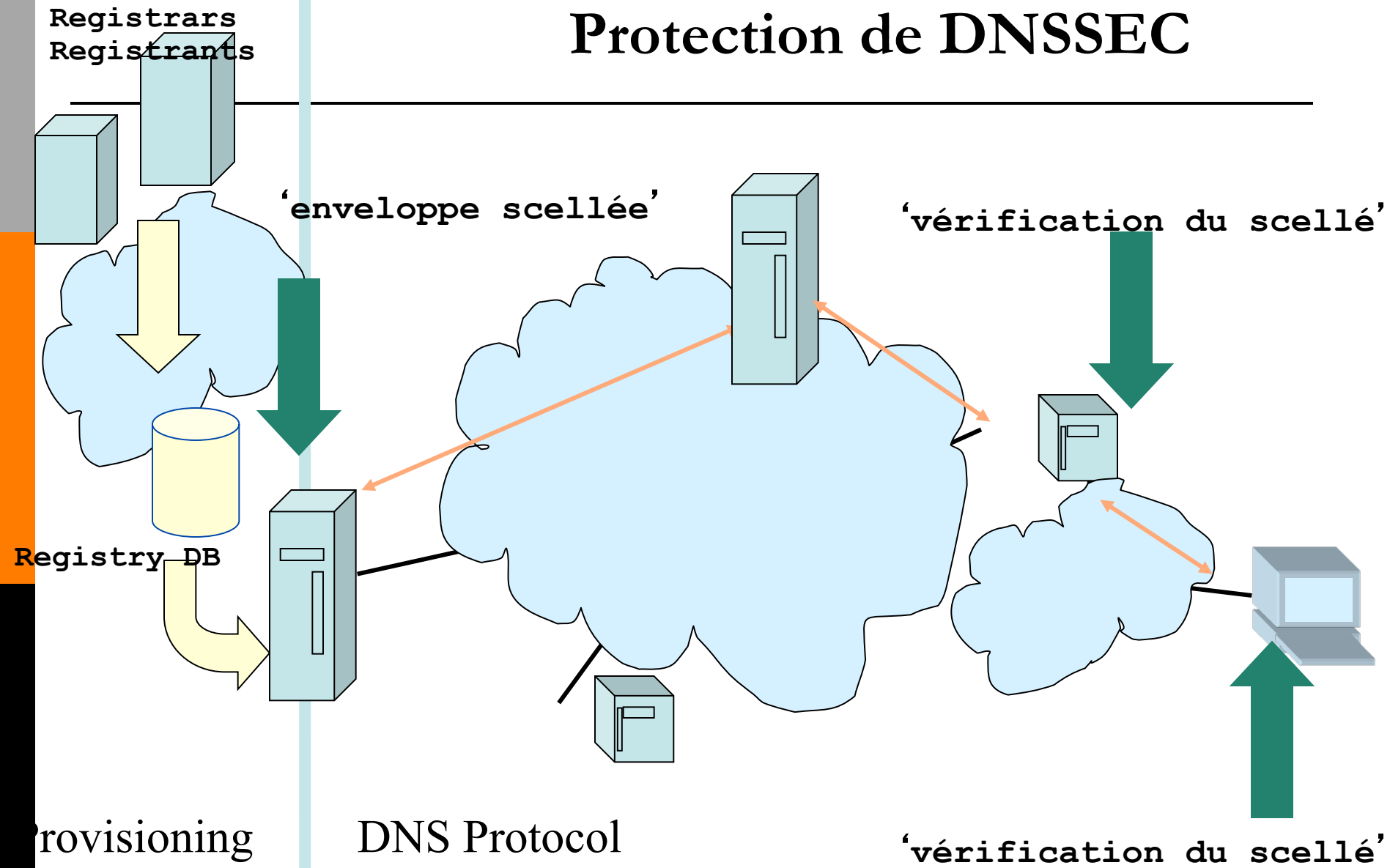
---

- DNSSEC fournit l'authentification de message et la vérification d'intégrité à travers des signatures cryptographiques
  - Source DNS Authentique
  - Pas de modifications entre signature et validation
- Il ne fournit pas d'autorisation
- Il ne prévoit pas la confidentialité

# Protection de DNSSEC



# Protection de DNSSEC



# Bienfaits secondaires du DNSSEC

---

- DNSSEC Fournit un chemin de confiance indépendant
  - La personne qui administre “https” est certainement différente de la personne qui fait “DNSSEC”
  - Les chaînes de confiance sont probablement différentes

# Bienfaits secondaires du DNSSEC (suite)

---

- Avec une plus grande confiance dans le DNS
  - On peut assurer des négociations et échanges de clés
    - Enregistrements SSHFP, IPSECKEY, X509 CERTS
    - Groupe de travail IETF DANE
      - <https://tools.ietf.org/wg/dane>

# Attaques contre les PKI

The screenshot shows a web browser window with the URL [http://threatpost.com/en\\_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911](http://threatpost.com/en_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911). The page is from Threatpost, titled "Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It". The article is by Dennis Fisher, dated August 29, 2011, at 7:31 PM. The main headline is "Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It". The article text states: "UPDATE: A certificate authority in the Netherlands issued a valid SSL wildcard certificate for Google to a third party in July, leading to concerns that attackers may have been using the certificate to route sensitive traffic through their own servers, capturing it and compromising user data in the process. The certificate was revoked by the CA, DigiNotar, after the problem came to light Monday and Mozilla and Microsoft both have removed DigiNotar from their lists of trusted root CAs. The attack appears to have been targeting Gmail users specifically. Some users trying to reach the Gmail servers over HTTPS found that their traffic was being rerouted through servers that shouldn't have been part of the equation. On Monday afternoon, security researcher Moxie Marlinspike checked the signatures on the certificate for the suspicious server, which had been posted to Pastebin and elsewhere on the Web, and found that the certificate was in fact valid. The attack is especially problematic because the certificate is a wildcard cert, meaning it is valid for any of Google's domains that use SSL. It's not clear who DigiNotar issued the certificate to at this point." The right sidebar features "Today's Most Popular" articles and a "Security for Virtualization" video advertisement.

Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It | threatpost

Router Allo...sco Systems Cisco IOS Se...sco Systems network aut...rche Google http://www...mniPCX.pdf ISOC-AU Submissions End-of-Sale...sco Systems Corporate ti...ncyclopedia

Attackers Obtain Valid Cert for G... Capture a Screen Shot with Mac OS X

The Kaspersky Lab Security News Service

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware  
Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home > SMB Security >

August 29, 2011, 7:31PM

## Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It

by Dennis Fisher

Follow @DennisF

Share Like 16

Comment

**UPDATE:** A certificate authority in the Netherlands issued a valid SSL wildcard certificate for Google to a third party in July, leading to concerns that attackers may have been using the certificate to route sensitive traffic through their own servers, capturing it and compromising user data in the process. The certificate was revoked by the CA, DigiNotar, after the problem came to light Monday and Mozilla and Microsoft both have removed DigiNotar from their lists of trusted root CAs.

The attack appears to have been targeting Gmail users specifically. Some users trying to reach the Gmail servers over HTTPS found that their traffic was being rerouted through servers that shouldn't have been part of the equation. On Monday afternoon, security researcher Moxie Marlinspike checked the signatures on the certificate for the suspicious server, which had been [posted to Pastebin](#) and elsewhere on the Web, and found that the certificate was in fact valid. The attack is especially problematic because the certificate is a wildcard cert, meaning it is valid for any of Google's domains that use SSL.

It's not clear who DigiNotar issued the certificate to at this point.

Security and privacy experts began discussing the problem Monday

Go to "http://threatpost.com/en\_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911"

### Today's Most Popular

- 60 Minutes Weighs Stuxnet's Legacy
- Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards
- NSA Develops New, Super-Secure Android Phone
- Threats From Third Party Vendors Demand Vigilance
- Former NSA Director Calls Stuxnet "Good Idea"

### Security for Virtualization

in 2 minutes

Get the right balance between security and performance with our animated video

> Watch the animation now

# Attaques contre les PKI(suite)

The screenshot shows a web browser window with the URL [http://threatpost.com/en\\_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611](http://threatpost.com/en_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611). The page header includes the Threatpost logo, the date "Monday, March 5th, 2012", and a search bar. Below the header is a navigation bar with categories like Apple, Cloud, Compliance, Critical Infrastructure, Cryptography, Government, Hacks, Malware, Microsoft, Mobile Security, SMB, Social Engineering, Virtualization, Vulnerabilities, and Web Security. The article title is "Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs" by Dennis Fisher, dated September 6, 2011, 1:37PM. The article text discusses the fallout from the DigiNotar compromise, mentioning that Microsoft revoked trust for five root certificates and Mozilla released new versions of Firefox. A sidebar on the right lists "Today's Most Popular" articles, including "60 Minutes Weighs Stuxnet's Legacy" and "Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards". At the bottom, there is a section titled "Security for Virtualization" with a video thumbnail and the text "Get the right balance between security and performance with our animated video".

Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs | threatpost

http://threatpost.com/en\_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611

Router Allo...sco Systems Cisco IOS Se...sco Systems network aut...rche Google http://www...mniPCX.pdf ISOC-AU Submissions End-of-Sale...sco Systems Corporate ti...ncyclopedia

Microsoft Revokes Trust in Five D... Capture a Screen Shot with Mac OS X

threatpost

Monday, March 5th, 2012

Google Custom Search Search

Newsletter Sign-up

The Kaspersky Lab Security News Service

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware

Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home > SMB Security >

September 6, 2011, 1:37PM

## Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs

by Dennis Fisher

Follow @DennisF

Share Like 5 0

1 Comment

The fallout from the [DigiNotar compromise](#) continued on Tuesday, as [Microsoft said it has now revoked its trust](#) of all five of the certificate authority's root certificates. The update that makes this change is being pushed out to users on all supported versions of Windows. Mozilla also released new versions of Firefox on Tuesday that revoke trust for all of DigiNotar's certificates.

The move by Microsoft effectively makes any certificate that has been issued by DigiNotar untrusted by Internet Explorer and other Windows applications. Any IE user who visits a site that presents a DigiNotar-issued certificate as proof of identity will get an error message telling him that the certificate isn't trusted. Microsoft's change applies to these root certificates from DigiNotar:

### Today's Most Popular

- 60 Minutes Weighs Stuxnet's Legacy
- Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards
- NSA Develops New, Super-Secure Android Phone
- Threats From Third Party Vendors Demand Vigilance
- Former NSA Director Calls Stuxnet "Good Idea"

### Security for Virtualization

in 2 minutes

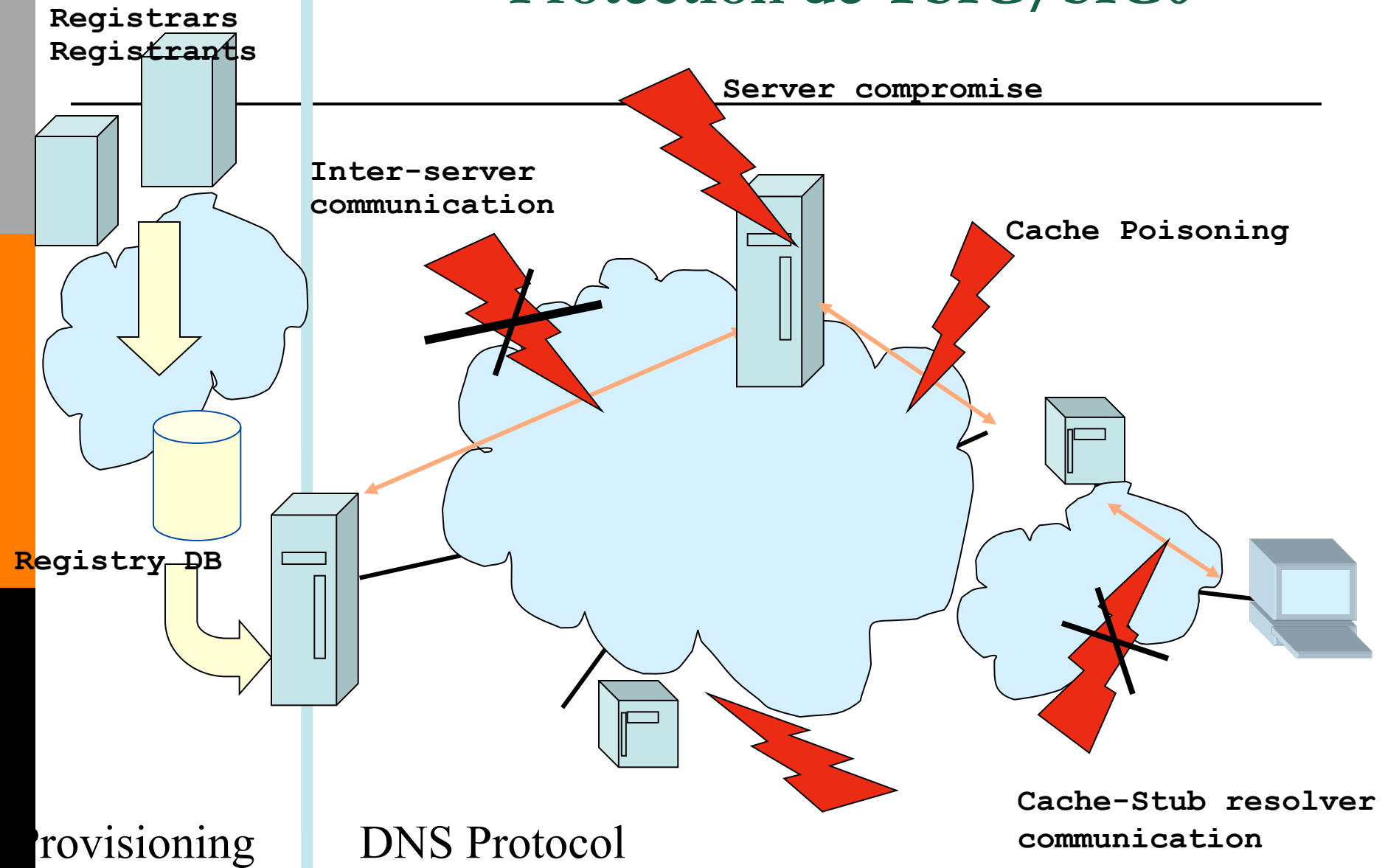
Get the right balance between security and performance with our animated video

# Autre mécanismes de sécurité DNS

---

- Nous avons parlé de la protection des données
  - La technologie de l'enveloppe scellée
- Il y a aussi la composante de sécurité du transport
  - Utile pour les communications bilatérales entre machines
  - TSIG ou SIG0

# Protection de TSIG/SIG0



# DNSSEC en une page

---

- L'authenticité et l'intégrité de données par la signature des ensembles de «resource Record » avec la clé privée
- La clé publique est utilisée pour vérifier les RRSIGs
- L'enfant signe sa zone avec sa clé privée
  - L'authenticité de cette clé est déterminée par la signature de contrôle du parent (DS)
- Cas idéal: une clé publique distribuée

# Authenticité et Intégrité

---

- Nous voulons vérifier l'authenticité et l'intégrité des données DNS
- Authenticité: Est ce la donnée publiée par l'entité supposée autoritaire ?
- Intégrité: Est ce la donnée reçue conforme à celle publiée ?
- La cryptographie à clé publique aide à répondre à ces questions
  - On peut utiliser les signatures pour vérifier l'intégrité et l'authenticité de donnée
  - On peut vérifier l'authenticité des signatures

# Cryptographie à clé publique

---

- Utilise deux clés : une privée et une publique
- Bref:
  - Si tu connais la clé publique, tu peux déchiffrer une donnée chiffrée avec la clé privée
    - **Signature et vérification de signature**
  - Si tu connais la clé privée, tu peux déchiffrer une donnée chiffrée avec la clé publique.
    - **Confidentialité**
- DNSSEC utilise seulement les signatures
  - PGP utilise les deux techniques

# Cryptographie à clé publique (suite)

---

- La sécurité du système de cryptographie est basée sur un tas d'équations mathématiques dont la résolution demande le parcours d'un grand espace de solution (*ex.* factorisation)
- Algorithmes : DSA, RSA, ECC, Gost etc..
- Les clés publiques ont besoin d'être distribuées.
- Les clés privées ont besoin d'être gardées secrètes
  - Pas évident
- La cryptographie à clé publique est 'lente'

# Nouveaux “ER” pour DNSSEC

---

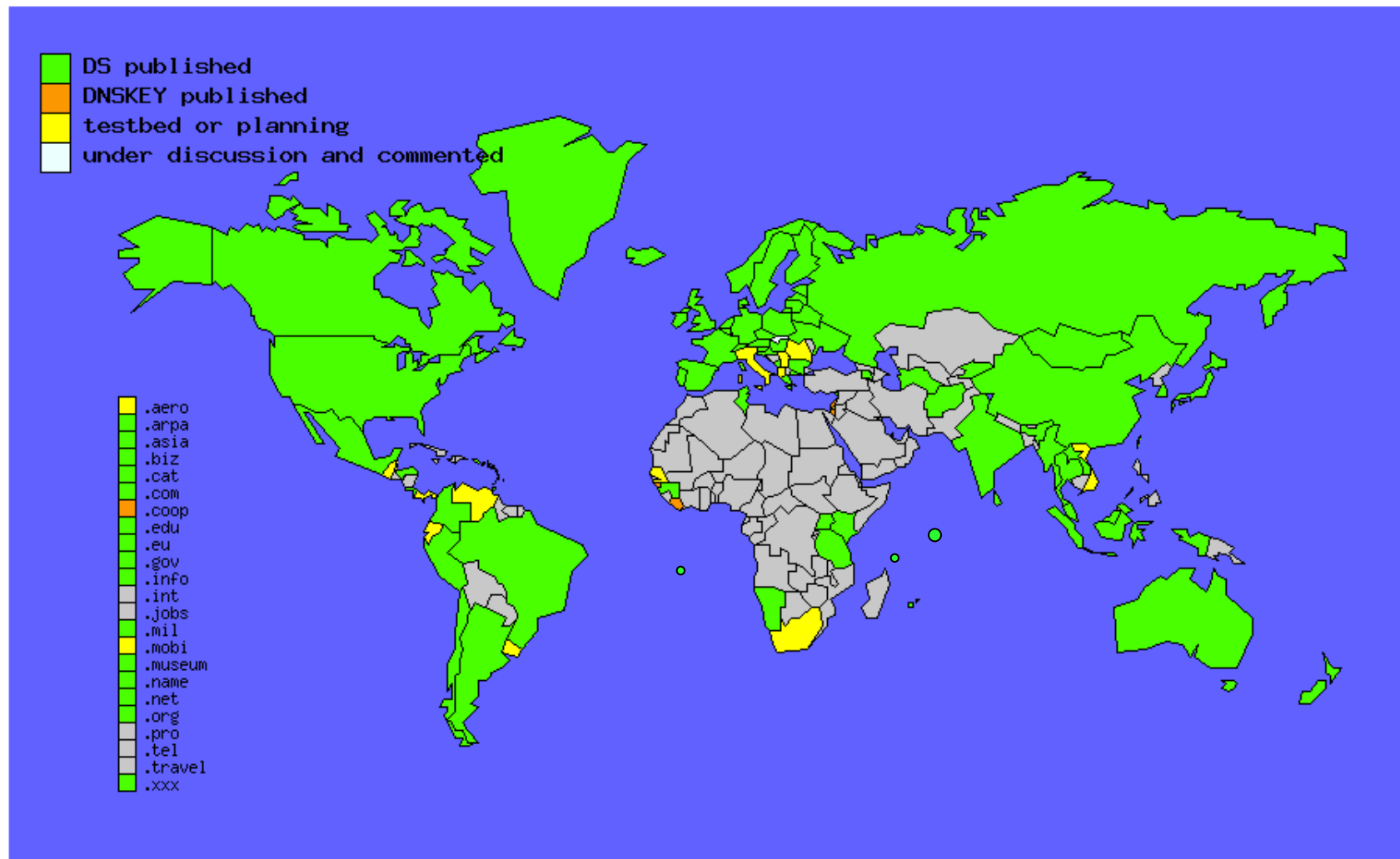
- 3 Enregistrements de Ressource à base de clé publique
  - RRSIG: Signature d'un “jeu” de ER faite avec la clé privée
  - DNSKEY: Clé publique, nécessaire pour la vérification d'un RRSIG
  - DS: Délégation Signer: ‘Pointeur’ de construction de chaîne de confiance

# Nouveaux “ER” pour DNSSEC (suite)

---

- 1 ER pour la consistance interne
  - NSEC: ER pour indiquer le nom suivant dans la zone et quel type de ER sont disponibles pour le nom actuel
    - **Authentifie la non existence de données**
- Pour des clés publiques non DNSSEC : X509/ IPSECKEY, SSHKEY....

# Adoption DNSSEC ccTLDs and gTLDs



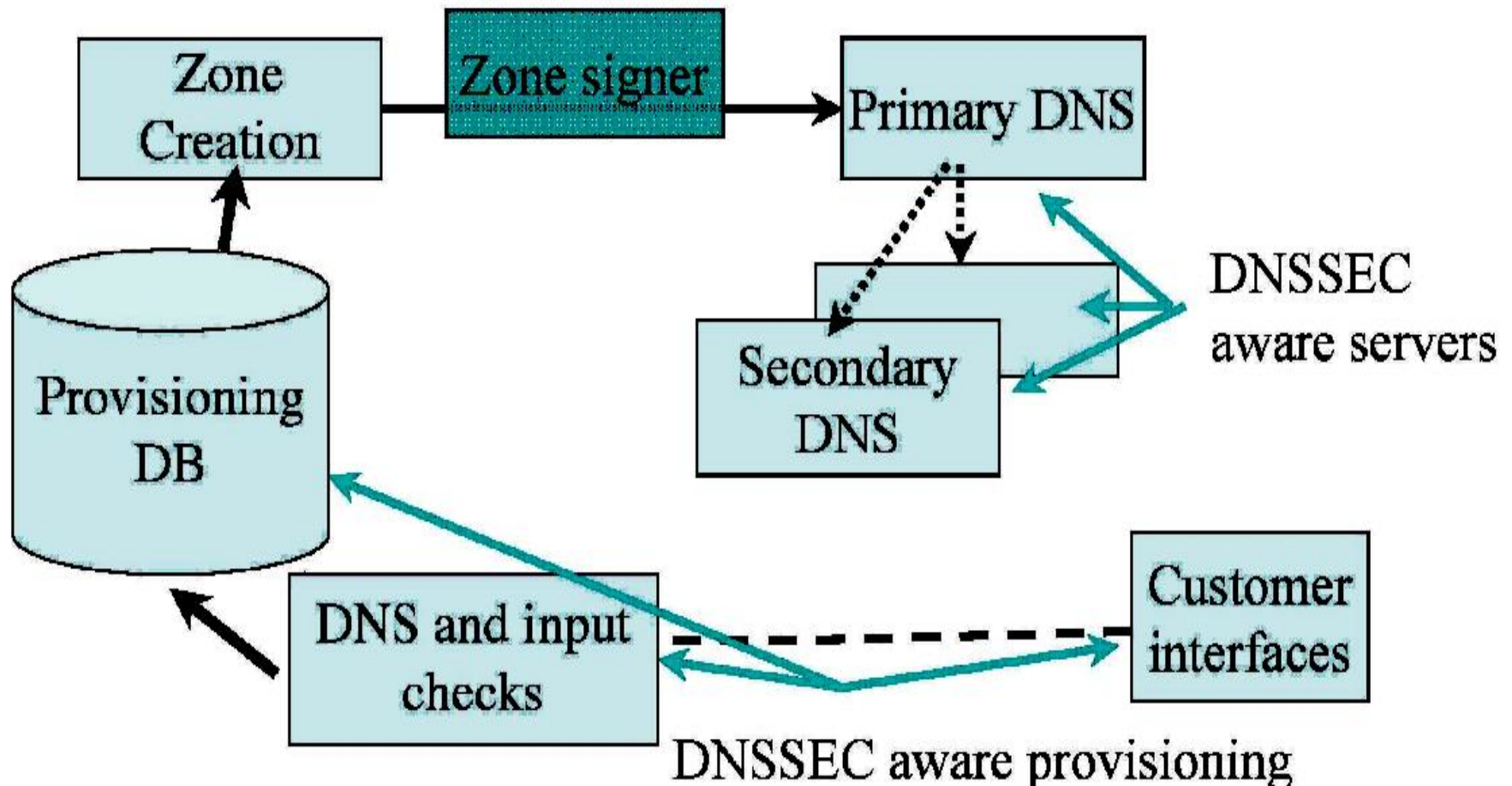
<http://www.ohmo.to/dnssec/maps/11/12/2015>

# Tâches de déploiement de DNSSEC

---

- Politiques et outils de gestion des clés
  - Utilisation et protection de la clé privée
  - Distribution de la clé publique
- Signature et Intégration de zone dans la chaîne d'approvisionnement
- Infrastructure de serveurs DNS
- Délégation sécurisée des modifications du registre
  - Interfaçage avec les clients

# Modification de l' Architecture DNSSEC

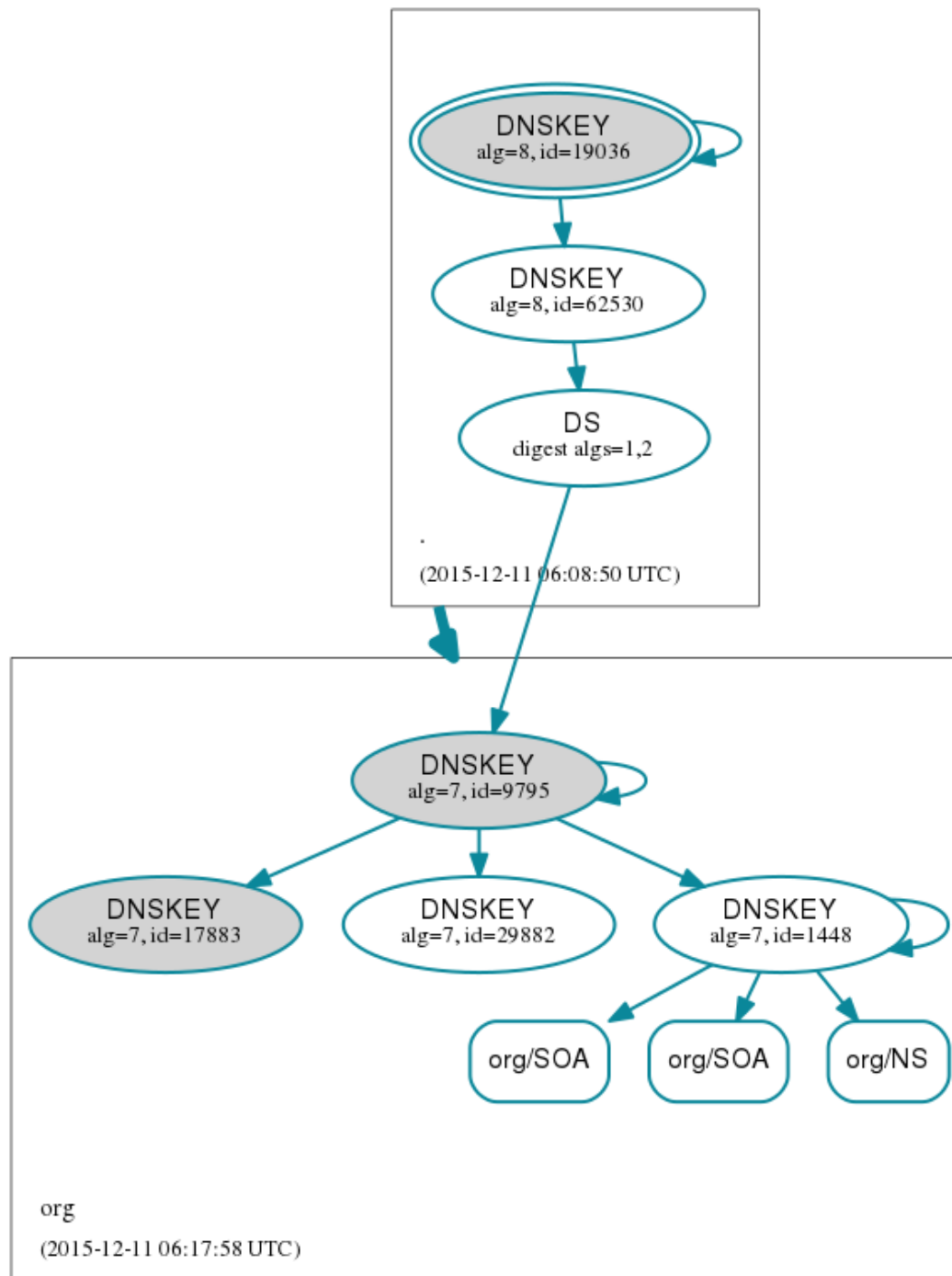


## La racine est signée

---

- Les validateurs ont besoin d'installer un Point d'entrée de sécurité (Trust Anchor) dans leurs logiciels
- La clé publique de la Racine
- <https://www.iana.org/dnssec>

dnsviz.net



# Quelques Hics avec DNSSEC

---

○ Ne protège pas contre les attaques de déni de service; mais en augmente les risques

- **Charge de travail cryptographique**
- **Longueur des message DNS**
- **RFC5358**

○ Ne protège pas les ERs non signés(données non autoritaires aux points de délégation)

- **NS et glue dans la zone parent**
- **Il faut protéger les transferts de zone par autres techniques**

# Quelques Hics avec DNSSEC (suite)

---

- DNSSEC introduit un mécanisme qui permet de lister tous les noms d'une zone en suivant la chaîne NSEC
  - **NSEC3** si le “zonewalk” est un problème pour vous
- Certains firewalls/middle box ne supportent pas des paquets DNS > 512 Octets(edns0)
  - **Beaucoup sont reconfigurables**
- Certains Firewalls/middle box ont des soucis avec les bits AD,CD,DO
- Certains vieux résolveurs peuvent avoir des soucis avec le bit AD

# Quelques Hics avec DNSSEC (fin)

---

- Ajoute de la complexité au DNS, augmentant ainsi les risques de mauvaises configurations
- Comment se fera la distribution et le renouvellement du Trust Anchor(KSK de la racine) ?
  - **RFC5011**

# Lectures

---

- <http://www.bind9.net/manuals>
- <http://www.dnssec.net>
- RFC (<http://www.rfc-editor.org>)
  - RFC 3833 (Vulnérabilités du DNS)
  - RFC 4033
  - RFC 4034
  - RFC4035
  - RFC4641
  - <http://tools.ietf.org/id/draft-ietf-dnsop-rfc4641bis-01.txt>

# Questions?

---

