



Tunisie-2015

Track SS-F : Services Internets évolutifs



AFRICA
INTERNET
SUMMIT '15
24 May to 5 June - Tunisia

DNSSEC

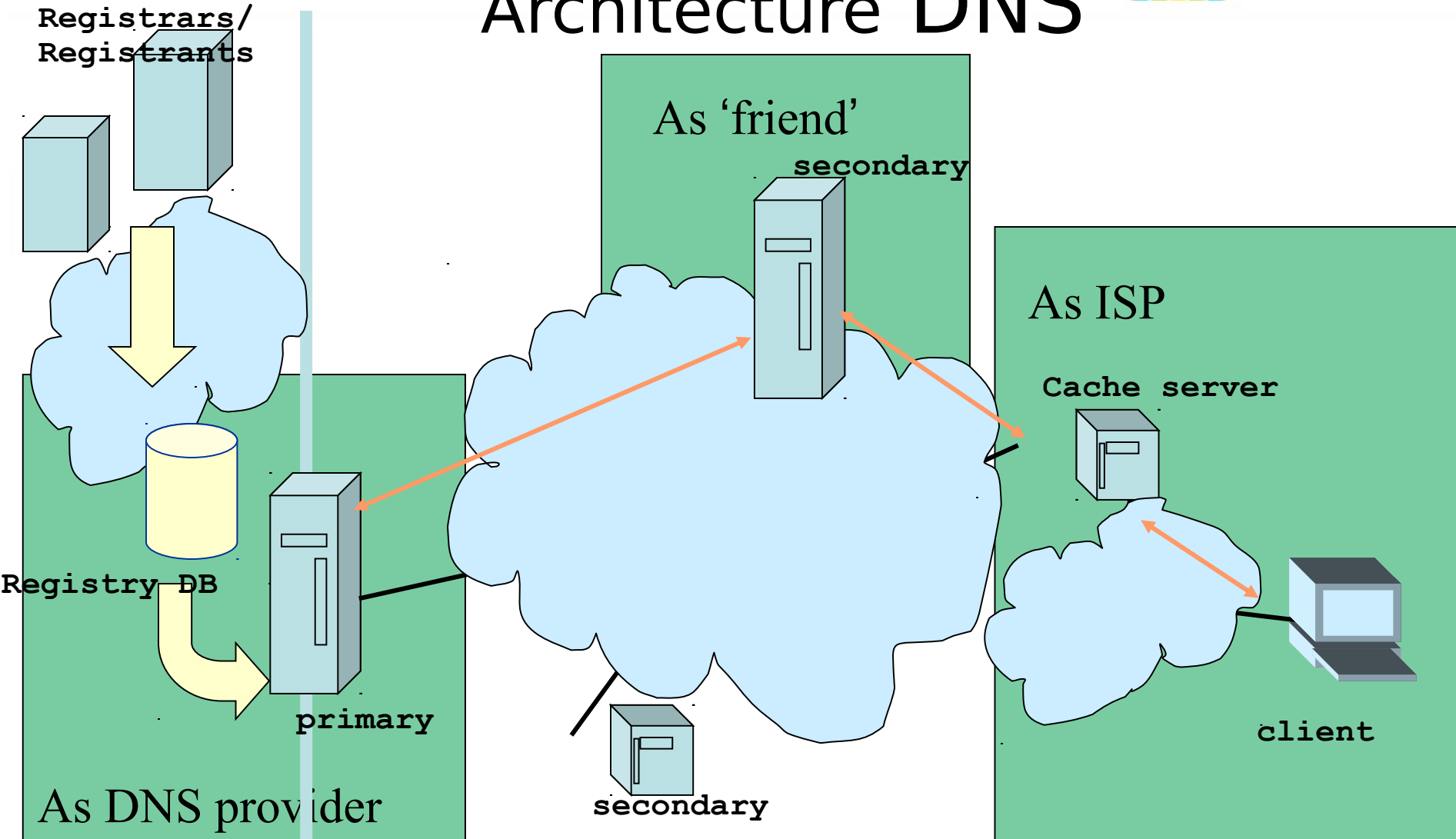
Pourquoi et détails du protocole

Alain Patrick AINA
aalain@trstech.net

AFNOG 2014, Djibouti, Djibouti



Architecture DNS

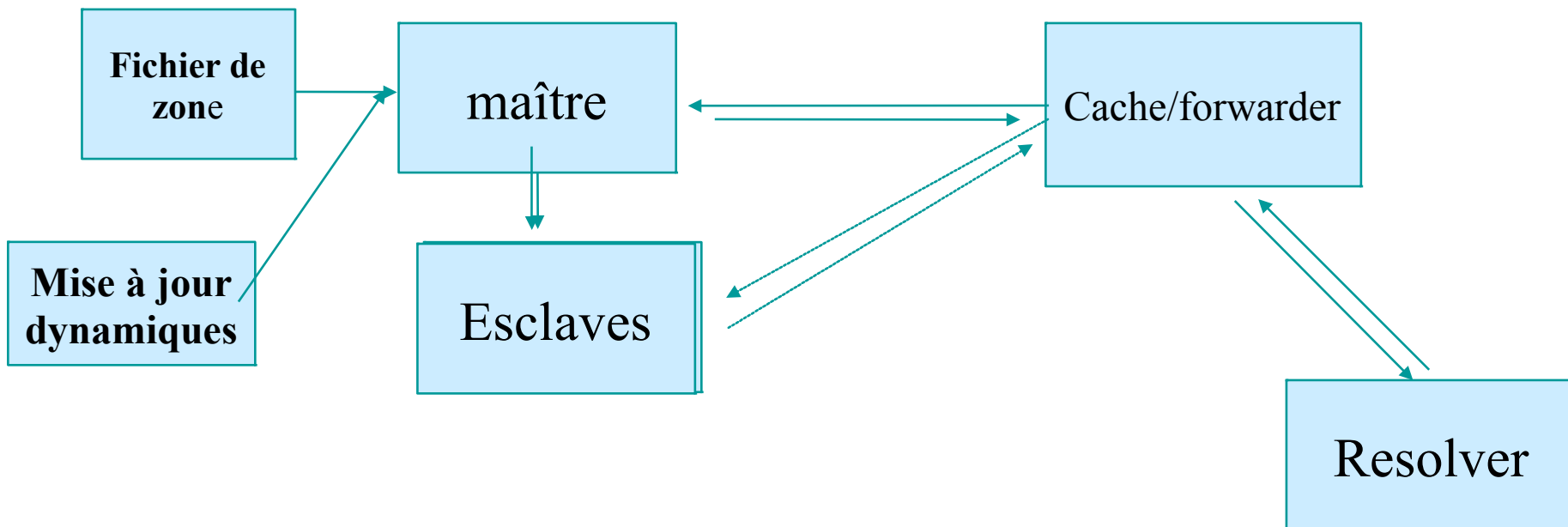


Provisioning

DNS Protocol

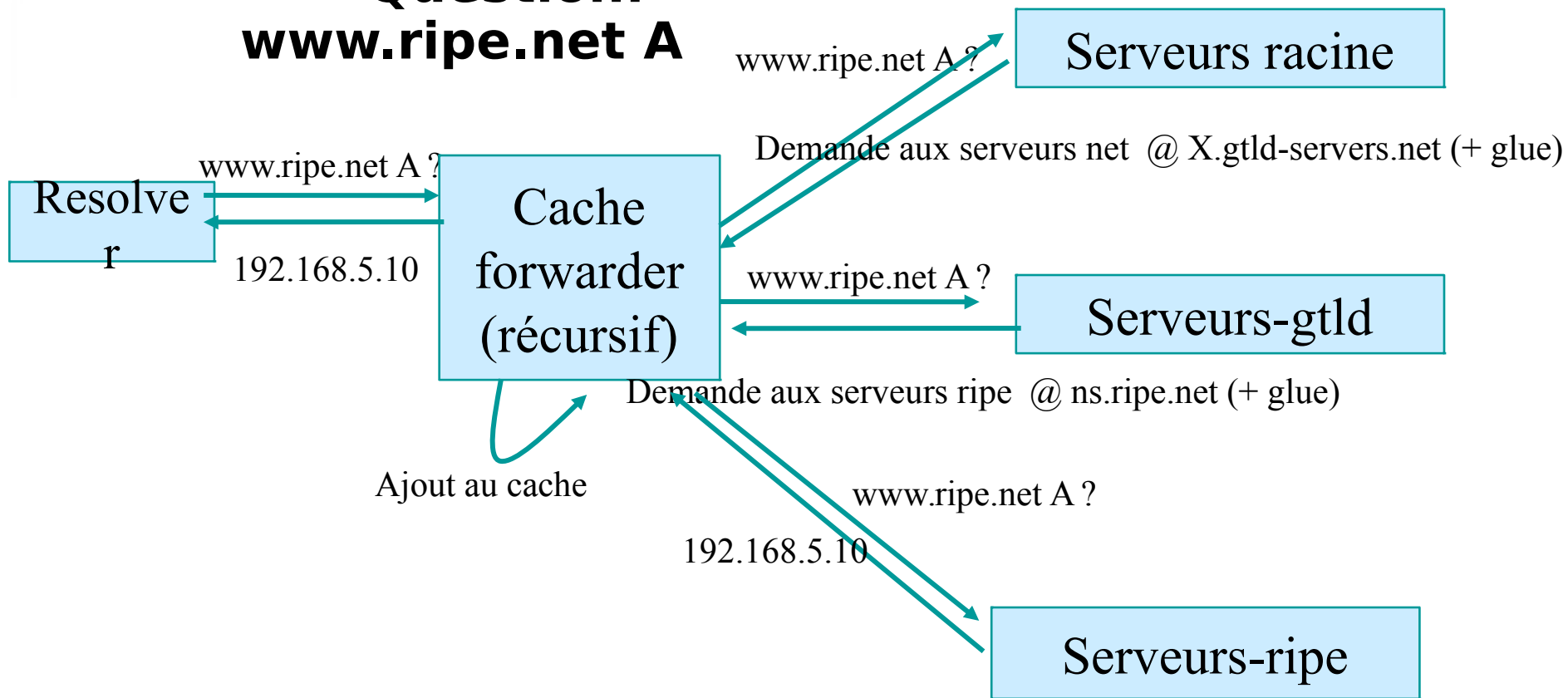


DNS Mouvement des données



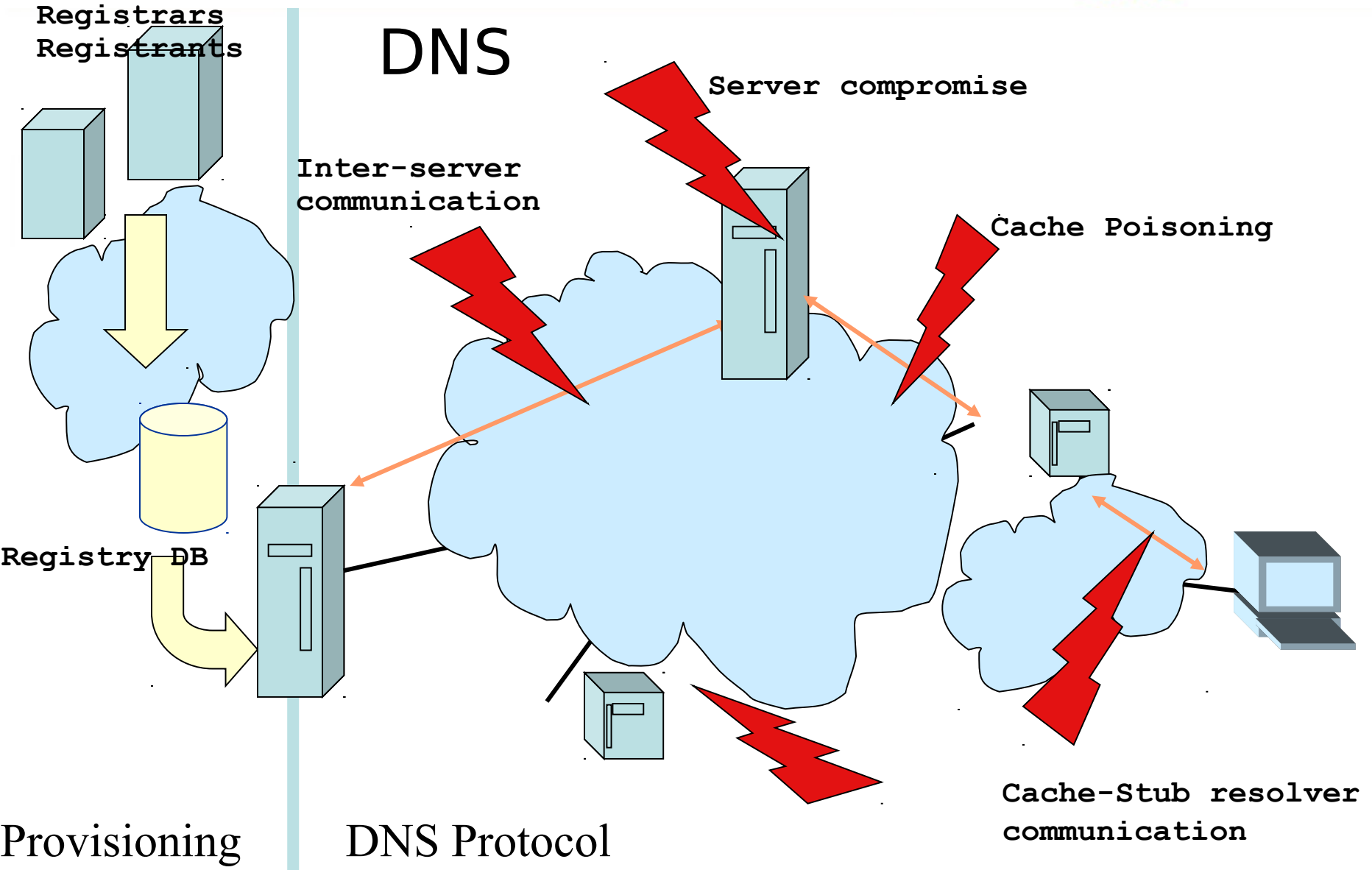
Résolution DNS

Question:
www.ripe.net A





DNS





Scan de mail non

Subject:
tenure

Surprisé

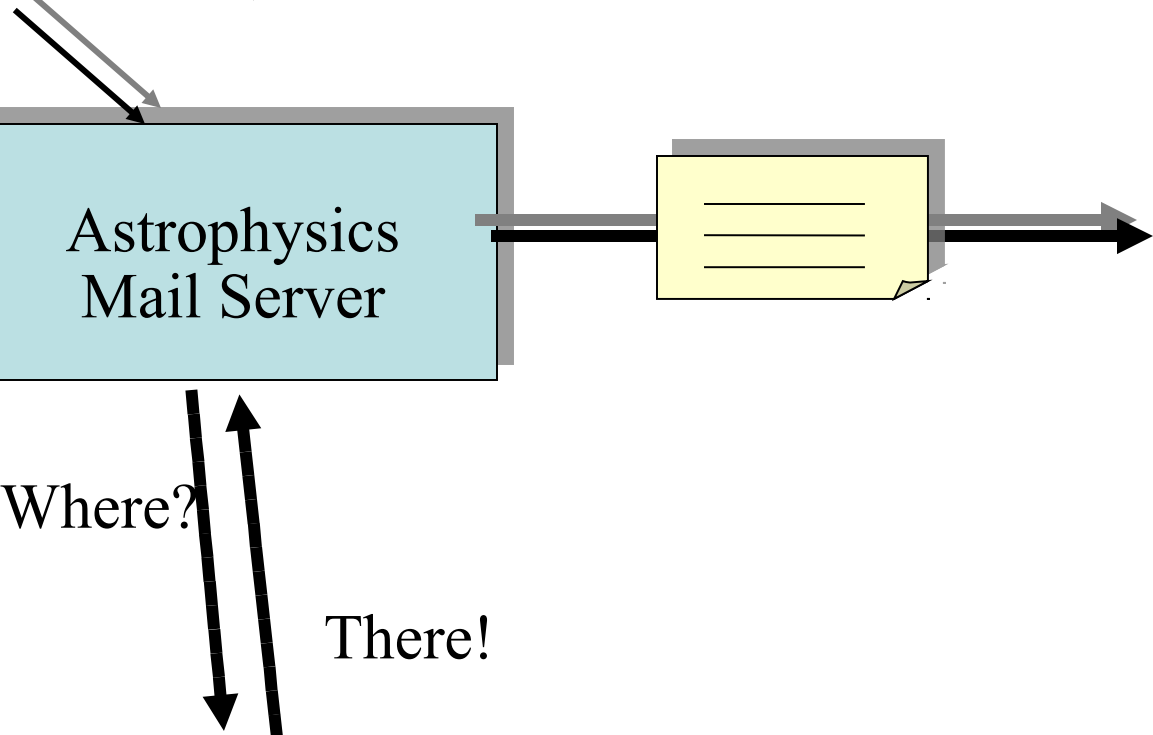
Astrophysics
Mail Server

Central Admin
Mail Server

Where?

There!

DNS

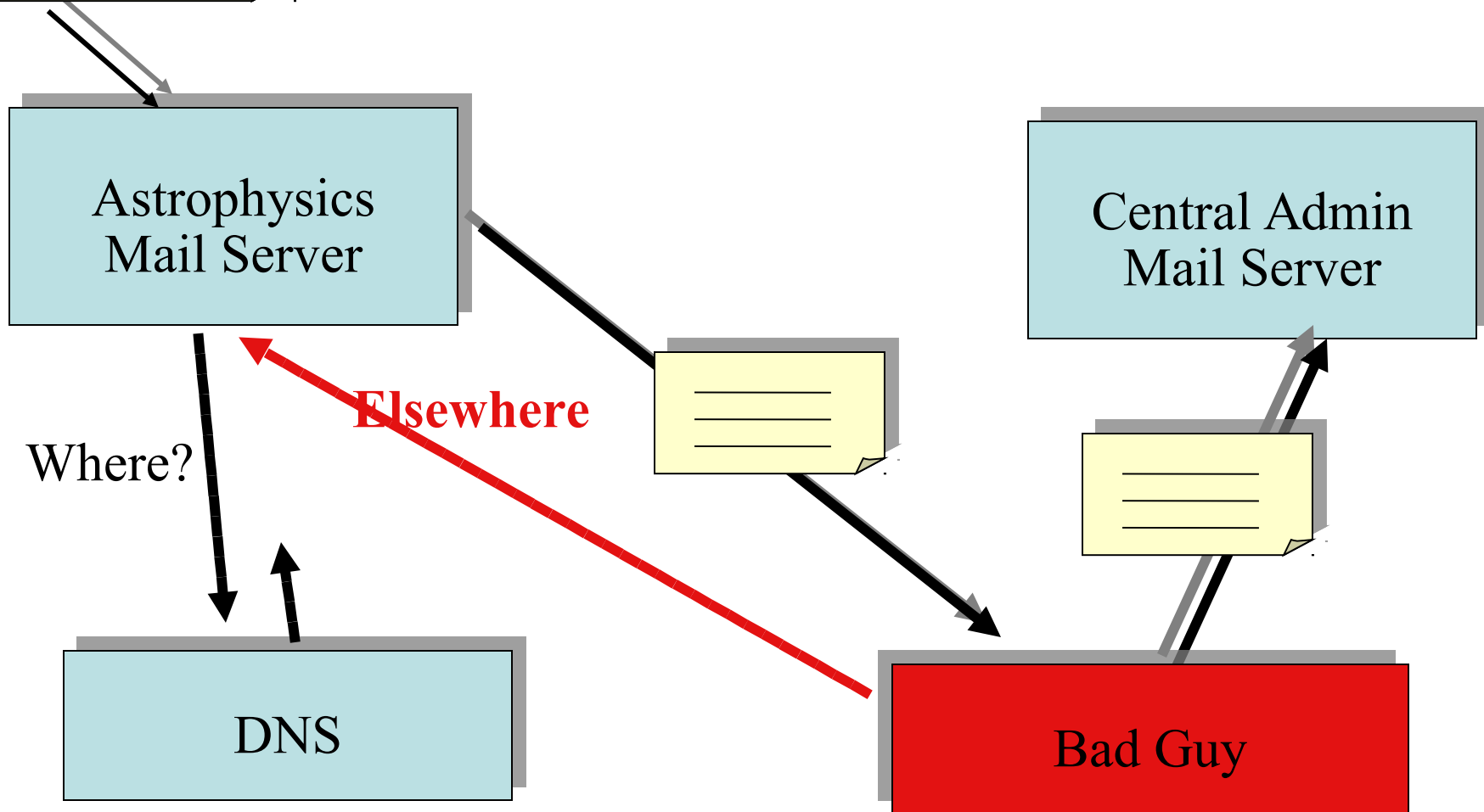




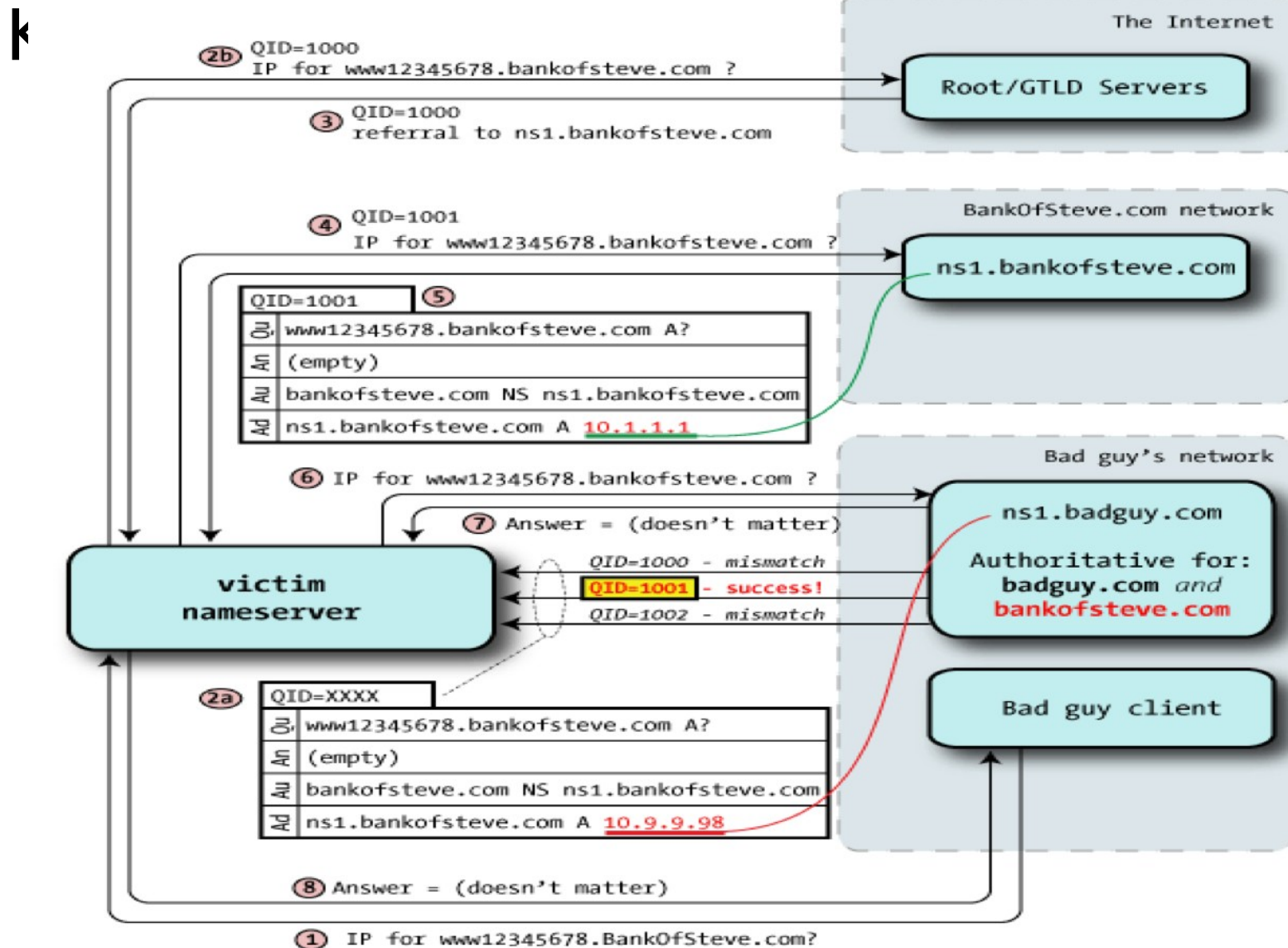
Scan de mail non

Subject:
tenure

orisé




Attaques de





Attaques de Kaminsky (suite)

Stay Updated | Metasploit Blog | Website Feedback

[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] caughq.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?

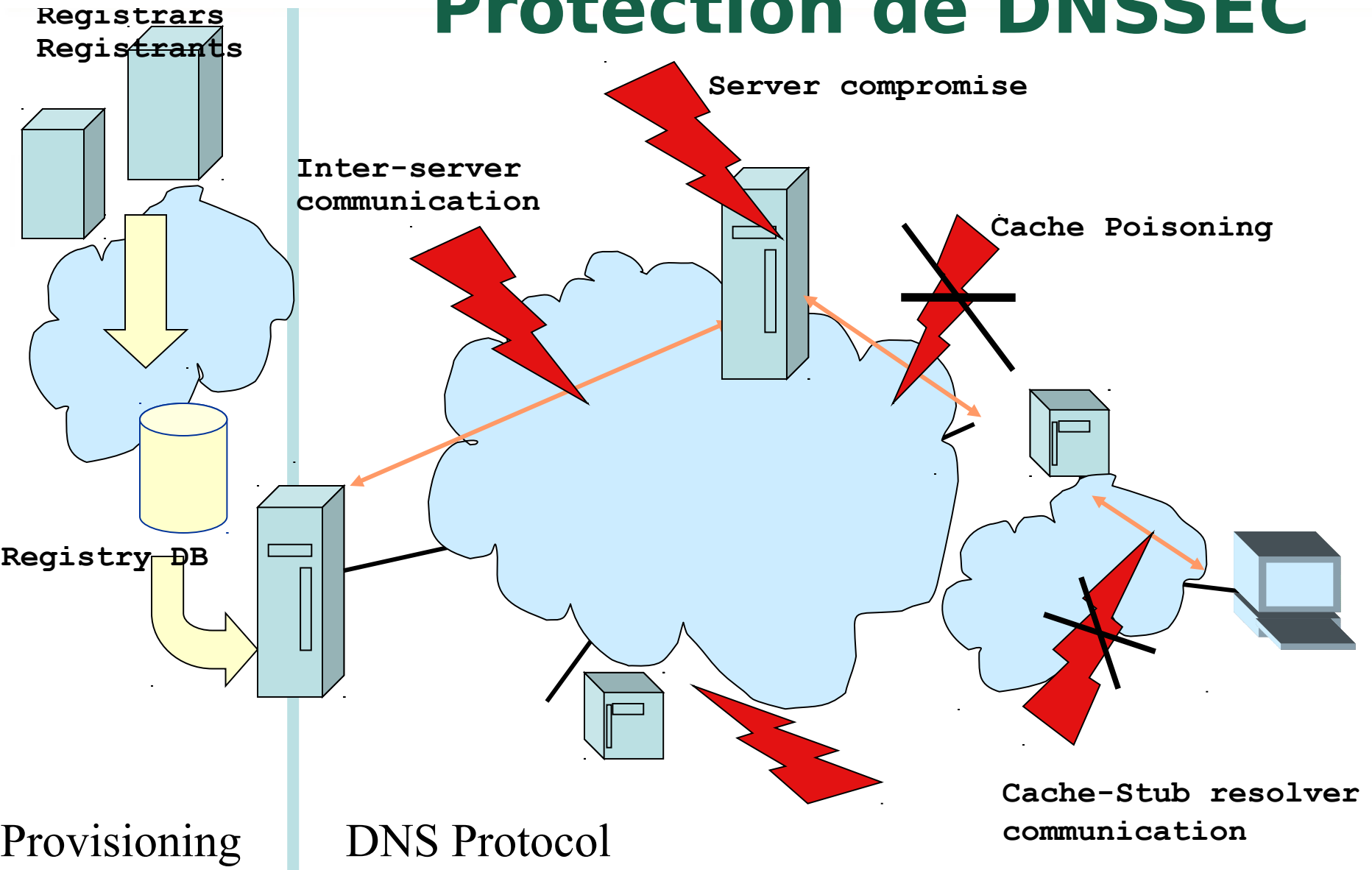
- DNSSEC sécurise le mappage des noms en adresses IP, etc...
 - La sécurité au niveau transport et applicatif est du ressort d'autres couches.

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



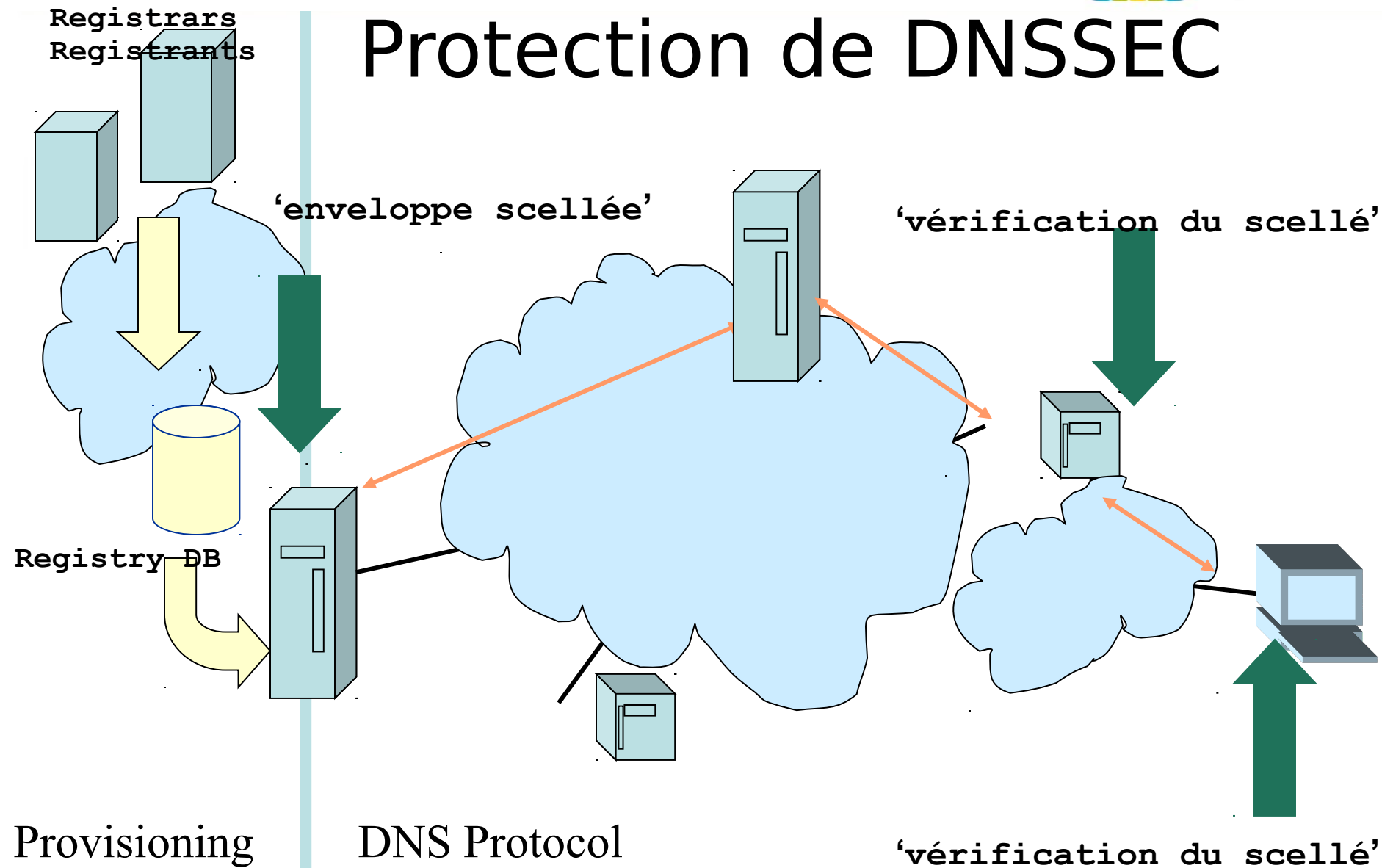
Provisioning

DNS Protocol

Cache-Stub resolver communication



Protection de DNSSEC



Bienfaits secondaires du DNSSEC

- DNSSEC Fournit un chemin de confiance indépendante
 - 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



Attaques contre les PKI

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

http://threatpost.com/en_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-08291

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

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

threat post Monday, March 5th, 2012

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 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

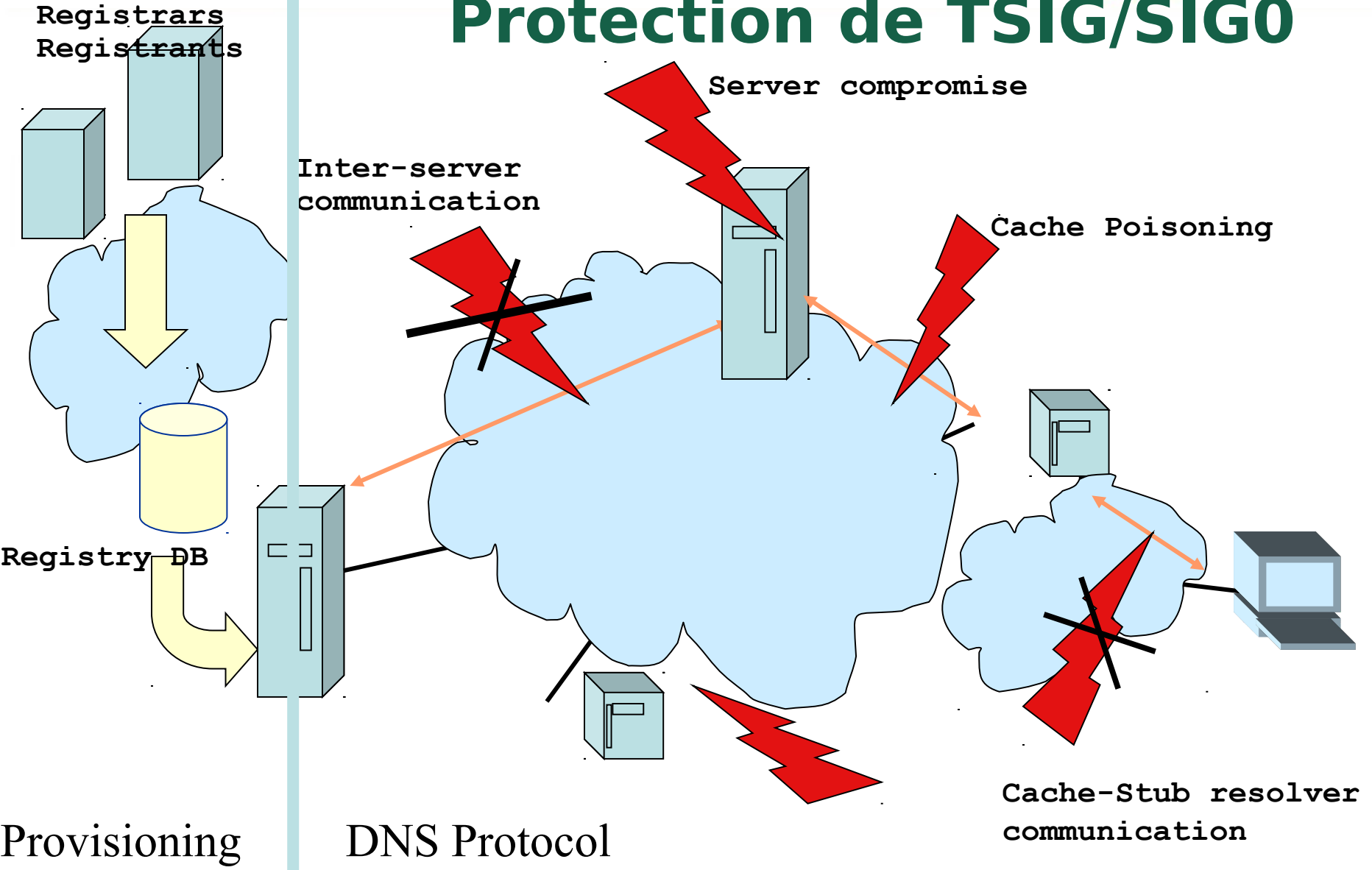
Get the right balance between security and performance with our animated video

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



Provisioning

DNS Protocol

Cache-Stub resolver communication



DNSSEC en une page

- L'authenticité et l'intégrité de données par la signature des ensembles de «ressource 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, elliptic curve, 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: Delegation Signer: ‘Pointeur’ de construction de chaîne de confiance
- 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 :
CERT/IPSECKEY(?)

ERs et “jeu” de ERs

- o Enregistrement de ressource:

- **label class ttl type rdata**

- ⌘ **www.ripe.net IN 7200 A 192.168.10.3**

- o Tout les ERs d’un “label” donné, “class”, “type” forment un “jeu” de ER:

www.ripe.net IN 7200 A 192.168.10.3
A 10.0.0.3

- o Dans DNSSEC, ce sont les “jeux” de ER qui sont signés et non les ERs individuels

RDATA de DNSKEY

- o 16 bits FLAGS → (0,256,257)
- o 8 bits protocole → (3: DNSSEC)
- o 8 bits algorithme → (1: RSA/MD5, 2: DH, 3: DSA, 4: Elliptic curve, 5: RSA/SHA1, etc...)
- o Clé publique à N*32 bits →

Exemples:

ripe.net. 3600 IN **DNSKEY** 256 3 5 (

AQOvhvXXU61Pr8sCwELcqqq1g4Jj

CALG4C9EtraBKVd+vGIF/unwigfLOA

O3nHp/cgGrG6gjYe8OWKYNgq3kDChN)

RSA/SHA-256 est recommandé comme remplaçant de RSA/SHA1



RDATA de RRSIG

- 16 bits type couvert
- 8 bits algorithmes
- 8 bits labels couvert
- 32 bit TTL original
- 32 bit expiration de signature
- 32 bit début de validité de signature
- 16 bit ID de clé
- Nom du signataire

```
www.ripe.net. 3600 IN RRSIG A 1 3 3600
20010504144523 (
    20010404144523 3112 ripe.net.
```

```
VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
```

```
vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
```

```
66DlubZDmNCXYw \
```

RDATA de NSEC

- Nom suivant dans la zone
- Liste également les types de ER existants pour un nom
- L'enregistrement NSEC du dernier nom pointe vers le premier nom dans la zone
- Exemple:

www.ripe.net. 3600 IN **NSEC** ripe.net. A RRSIG
NSEC

Enregistrement NSEC

- Authentification de la non-existence de “type” et de “labels”
Exemple de la zone ripe.net (Sans les RRSIG):

```

ripe.net.      SOA      .....
               NS      NS.ripe.net.
               DNSKEY  .....
               NSEC    mailbox DNSKEY NS NSEC RRSIG SOA
mailbox       A      192.168.10.2
               NSEC    www A NSEC RRSIG
www           A      192.168.10.3
               NSEC    ripe.net A NSEC RRSIG
  
```

dig smtp.ripe.net donnerait: **aa RCODE=NXDOMAIN**

autorité: mailbox.ripe.net. NSEC www.ripe.net. A NSEC RRSIG

dig www.ripe.net MX donnerait: **aa RCODE=NO ERROR**

autorité: www.ripe.net. NSEC ripe.net. A NSEC RRSIG

Delegation Signer: DS

- Indique que la zone déléguée est numériquement signée
- Essentiellement un pointeur vers la clé suivante dans la chaîne de confiance
- Le Parent est autoritaire pour le DS des zones enfant
- **Le DS ne doit pas être publié dans la zone enfant.**
- Règle beaucoup de problèmes
 - Renouvellement de clés

Delegation Signer: DS

(suite)

- DS : Le parent donne l'autorité de signer les ERs de la zone enfant en utilisant le DS
- Est un pointeur vers la prochaine clé dans la chaîne de confiance
 - Tu fais confiance à une donnée qui est signée en utilisant une clé vers laquelle pointe le DS

RDATA du DS

- o 16 bits ID de la clé de l'enfant
- o 8 bits algorithmme
- o 8 bits type de digest
- o XX octets de digest

Ce champ indique la clé suivante dans la chaîne de confiance

```
$ORIGIN ripe.net.
```

```
disi.ripe.net      3600 IN      NS      ns.disi.ripe.net
```

```
disi.ripe.net.    3600 IN      DS      3112  5 1 (
```

```
239af98b923c023371b521g23b92da1
```

```
2f42162b1a9
```

```
)
```


Signature de zone

- La signature accomplit les taches suivantes
 - Trier la zone
 - Insérer les enregistrement NSEC
 - Insérer RRSIG contenant une signature pour chaque “jeu” d’enregistrement de ressource.

La signature est faite avec la clé privée



Délégation de zone signée

- Le Parent signe l'enregistrement DS pointant vers un ensemble de clés de signature de clés

```

$ORIGIN net.

kids NS    ns1.kids
      DS   (...) 1234
      RRSIG DS (...)net.
money NS   ns1.money
      DS   (...)
      RRSIG DS
(...)net.
  
```

```

$ORIGIN kids.net.

@ NS    ns1.kids
  RRSIG NS (...) kids.net.
  DNSKEY (...) (1234)
  DNSKEY (...) (3456)
  RRSIG DNSKEY ... 1234 kids.net ...
  RRSIG DNSKEY ... 3456 kids.net ...

beth A 127.0.10.1
      RRSIG A (...) 3456 kids.net. ...
ns1  A 127.0.10.3
      RRSIG A (...) 3456 kids.net.
  
```

Clé de signature de clé

Clé de signature de zone

...

KSK/ZSK

- Deux différentes clés sont utilisées
- DS pointe vers la clé de signature de clé(KSK)
- Le KSK signe les clés
- La zone est signée avec la clé de signature de zone(ZSK)
- KSK peut être plus grande avec une grande durée de vie
- ZSK peut avoir une durée de vie courte
 - Peut être “petit” = “rapidité”

KSK/ZSK

- draft-ietf-dnsop-rfc4641bis-01.txt suggère
 - 1024 bits par défaut
 - 2048 pour les niveaux Trust Anchor ou clés difficiles à changer
 - RSA/SHA-256 dès que possible
 - Utiliser Une bonne source de nombre aléatoire
 - RFC4086
 - NIST SP 800-90
 - Renouvellement des KSK chaque 12 mois, même si elles sont valides pour 2 décennies
 - Renouvellement de ZSK chaque mois

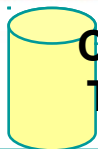


Chaîne de confiance

- Les données dans les zones peuvent être valides si elles sont signées par une ZSK
- La ZSK ne peut être valide que si elle est signée par une KSK
- La KSK ne peut être digne de confiance que si elle est référencée par un enregistrement DS de confiance
- Un enregistrement DS ne peut être valide que s'il est signé par la ZSK du parent ou
- Une KSK peut être valide si elle est échangée hors bande (Trusted key)



Chaîne de confiance



Configuration locale

Trusted key: . 8907 \$ORIGIN .

Clé de signature de zone

Clé de signature de clé

\$ORIGIN net.

```

. DNSKEY (...) lasE5... (2983)
  DNSKEY (...) 5TQ3s... (8907)
  RRSIG KEY (...) 8907 . 69Hw9..

net. DS 7834 3 1ab15...
  RRSIG DS (...) . 2983

```

```

net. DNSKEY (...) q3dEw... (7834)
  DNSKEY (...) 5TQ3s... (5612)
  RRSIG KEY (...) 7834 net. cMaso3Ud...

```

\$ORIGIN ripe.net.

```

ripe.net. DS 4252 3 1ab15...
  RRSIG DS (...) net. 5612

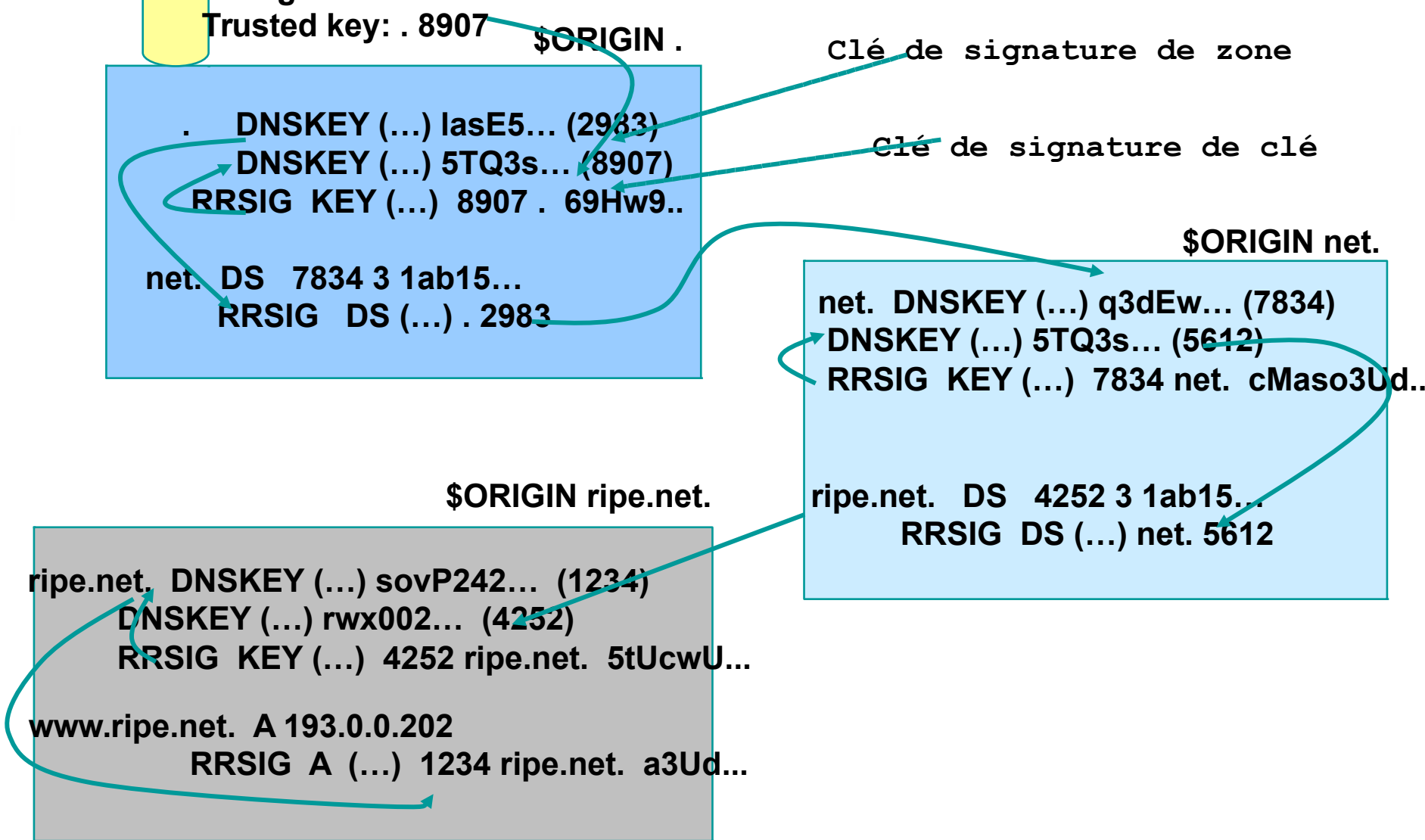
```

```

ripe.net. DNSKEY (...) sovP242... (1234)
  DNSKEY (...) rwx002... (4252)
  RRSIG KEY (...) 4252 ripe.net. 5tUcwU...

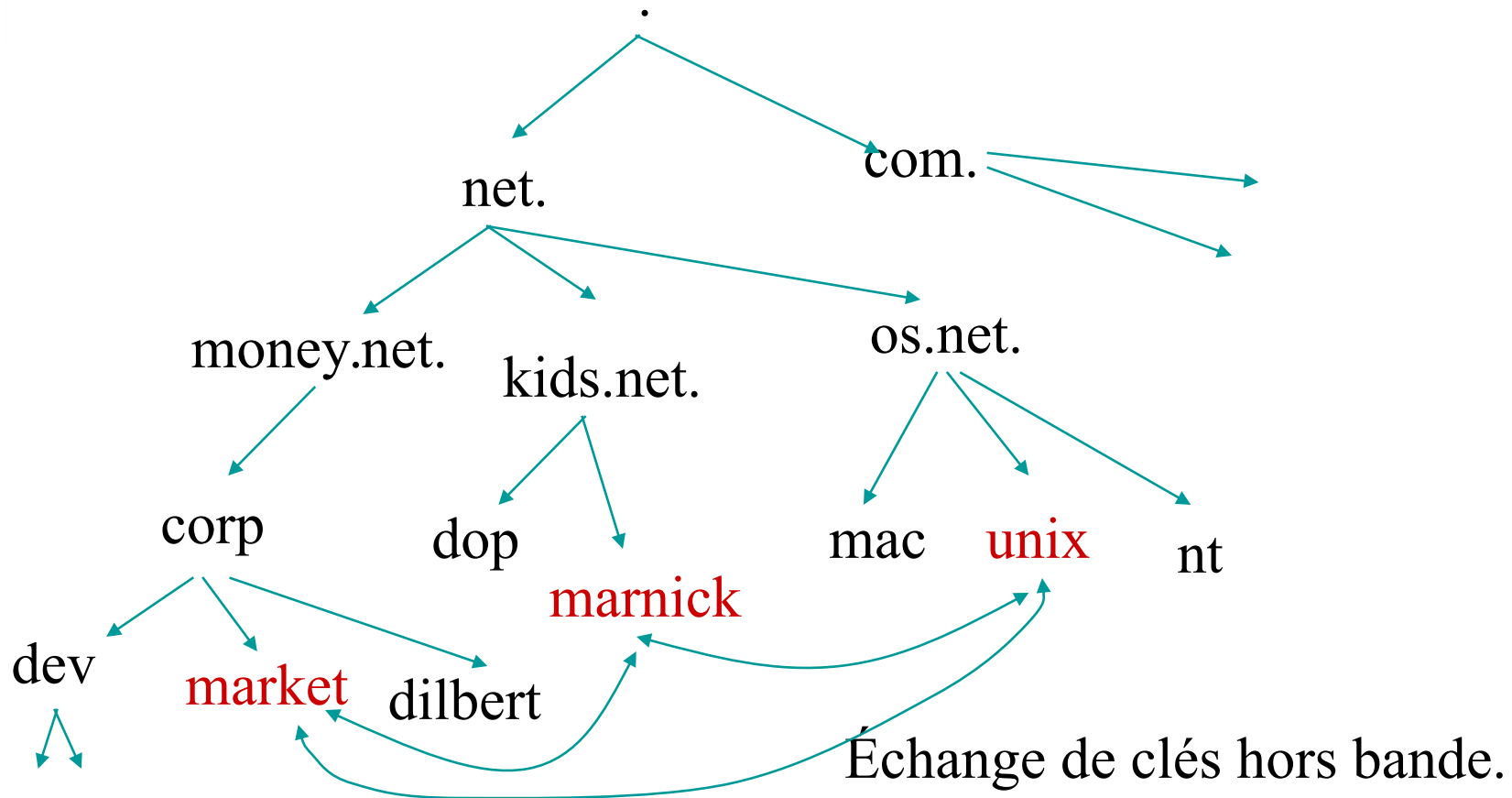
www.ripe.net. A 193.0.0.202
  RRSIG A (...) 1234 ripe.net. a3Ud...

```



Sécurisation de l'arborescence du DNS

- o Problème de distribution de clés



Des zones non sécurisées

- L'évidence cryptographique de l'état non sécurisé d'une zone est fournie par le parent
- S'il n'y a pas d'enregistrement DS, comme prouvé par un enregistrement NSEC avec une signature valide, l'enfant n'est pas sécurisé.
- Un enfant peut contenir des signatures, mais celles-ci ne seront pas utilisées pour construire une chaîne de confiance

Bit AD

- Un bit d'état dans la section « header » des paquets DNS
 - Non utilisé avant DNSSEC(devrait être à zéro)
 - Utilisé uniquement dans les réponses d'un serveur de validation
- Le bit AD n'est pas positionner par un serveur autoritaire sauf pour des données qu'il contrôle et s'il est configuré pour..
- AD = Authenticated data(donnée authentique)

Bit CD

- Un bit d'état dans la section « header » des paquets DNS
 - Non utilisé avant DNSSEC(devrait être à zéro)
- CD = Checking Disable (validation désactivée)
 - 1= validation désactivée
 - Le “resolver” accepte des réponses non vérifiées
 - 0= validation activée
 - Le “resolver” veut des réponses vérifiées pour les données signées,mais accepte les réponses non vérifiées pour les données non signées

Bit D0

- Un bit d'état dans la section « header » des paquets DNS
 - Non utilisé avant DNSSEC (devrait être à zéro)
 - 1= le “resolver” veut les enregistrements DNSSEC
 - 0= le “resolver” ne veut pas les enregistrements DNSSEC

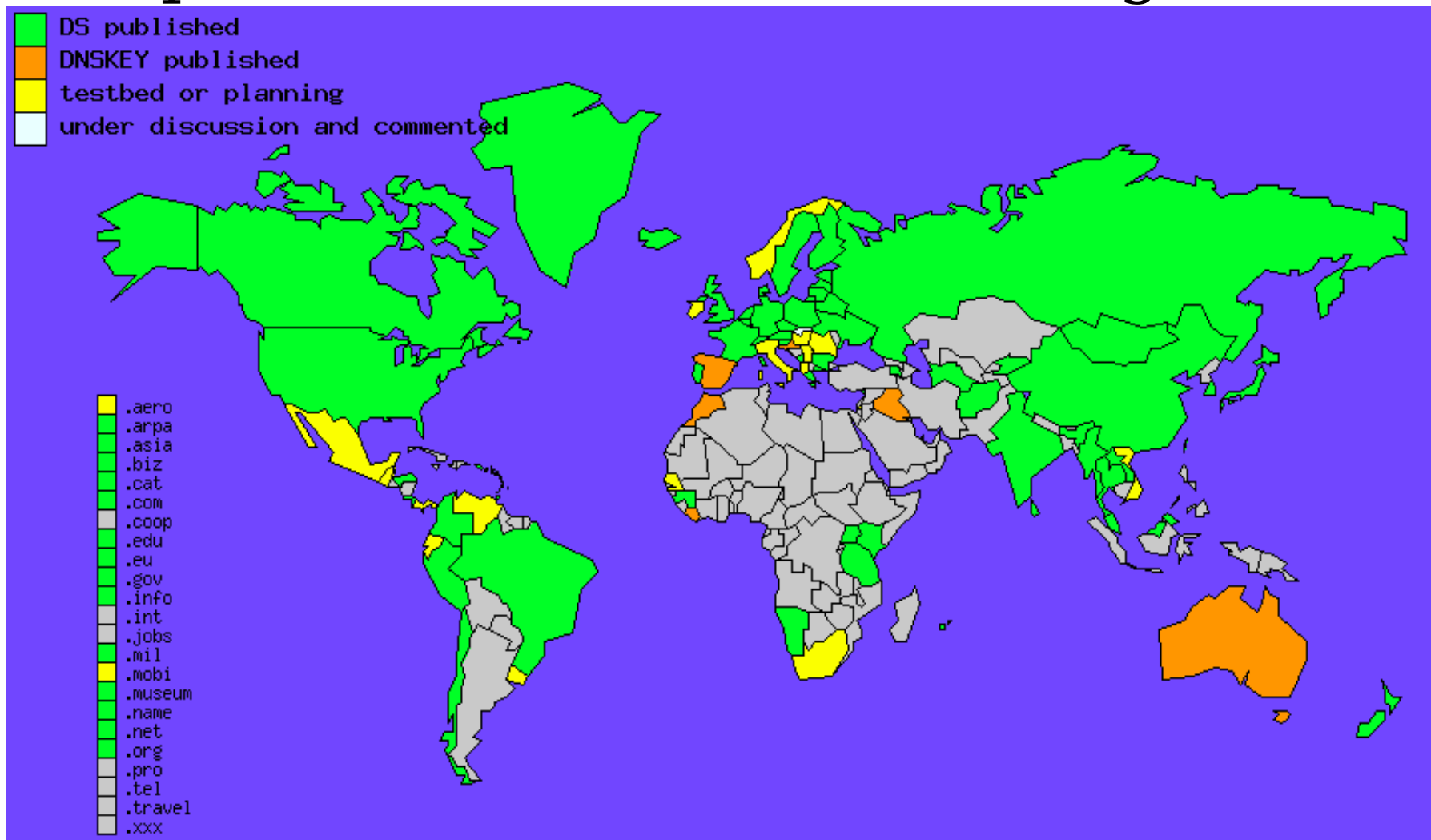
Utilisation du DNS pour distribuer les clés

- Les îles sécurisées rendent problématique la distribution de clés
 - Distribution de clés par le biais du DNS:
 - Utiliser une clé de confiance pour établir l'authenticité des autres clés
 - Construire des chaînes de confiance de la racine vers le bas
 - Les parents ont besoin de signer les clés de leurs enfants
 - Seul la clé racine est nécessaire dans un monde idéal
 - Les parents délèguent toujours la sécurité à l'enfant
- ... Mais il n'est pas intéressant de signer votre zone si le parent ne signe pas ou n'est pas signé ...

Utilisation du DNS pour distribuer les clés

- Construction des chaînes de confiance de la racine vers le bas de l'arborescence DNS
 - Outils:
 - ERs: DSNKEY, RRSSIG, DS, NSEC
 - Configuration manuelle des clés de la racine

Adoption DNSSEC ccTLDs and gTLDs

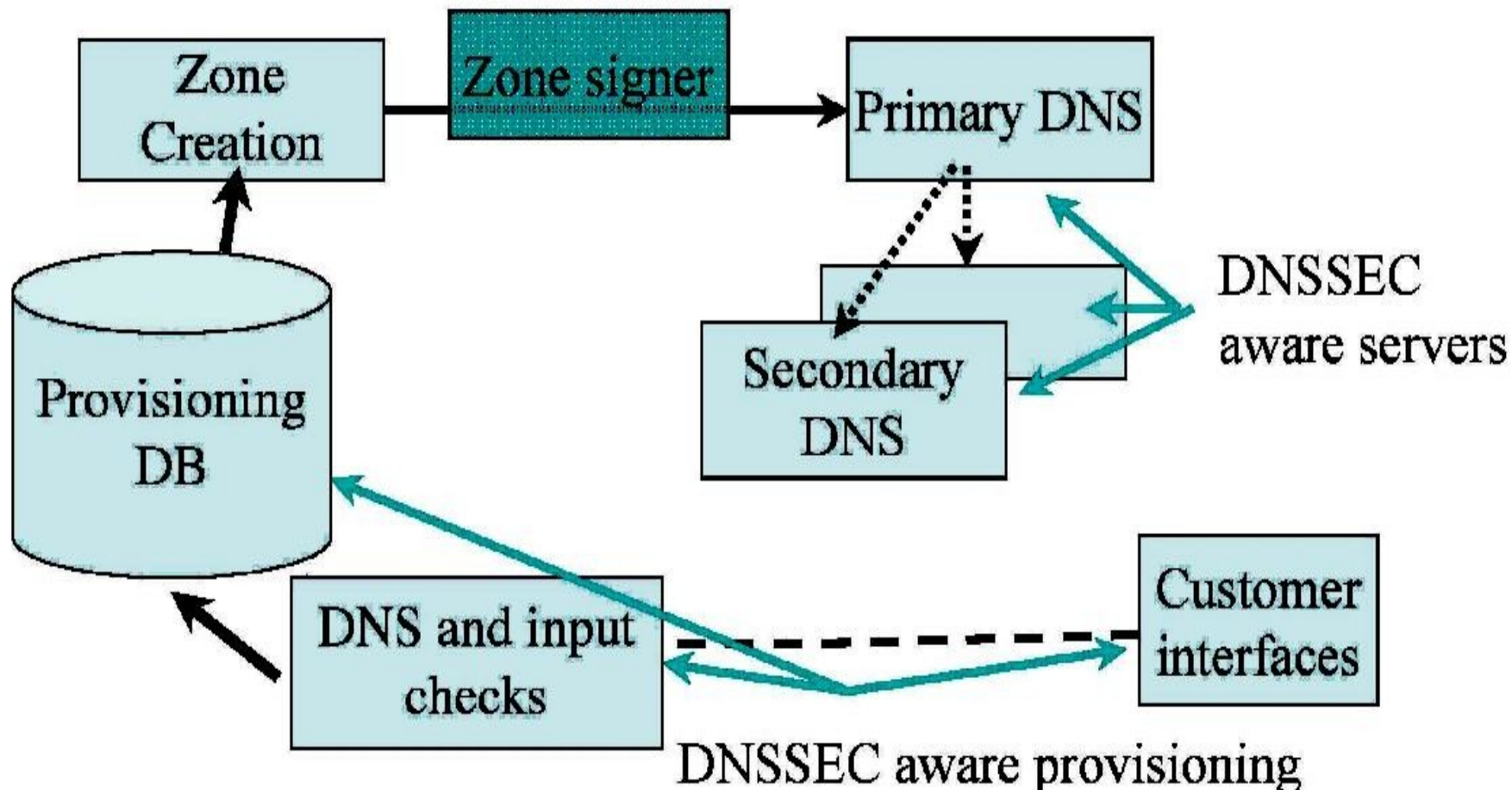


<http://www.ohmo.to/dnssec/maps/> 28/05/2014

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



o RENOUELEMENT DE CLES

CLES PRIVEES

- Vous devez garder votre clé privée secrète
- La clé privée peut être compromise
 - Mettre la clé sur une machine isolée derrière pare-feu et un contrôle d'accès solide
- Reconstruction de clé privée (Analyse de cryptographie)
 - Nombre aléatoire pas vraiment aléatoire
 - Défaillance du matériel de clé
 - Attaques brutales

RENOUVELLEMENT DE CLES

- Minimiser l'impact
 - Courte validité des signatures
 - Renouvellement régulier des clés
- NB: Les clés n'ont pas de tampons horaires en elles;
Les RRSIG sur les clés ont des tampons horaires
- La renouvellement de clés implique d'autres parties
 - L'état doit être maintenu pendant le renouvellement
 - pas toujours flexible
-

RENOUVELLEMENT DE CLES (suite)

- Avec la distinction de ZSK du KSK, il est maintenant possible de remplacer le ZSK sans affecter le parent
 - Il suffit seulement de re-signer le « jeu » ER du DNSKEY avec le KSK inchangé.
- Ceci est une forme de renouvellement de clé
 - On peut aussi remplacer le KSK
- Il est nécessaire d'avoir temporairement les deux clés (ancienne et nouvelle) présentes dans la zone
 - Assurer la transition
 - Jusqu'à expiration des RRSIG générées par l'ancienne clé



CHANGEMENT DE CLES NON PROGRAMME

- A besoin de communication hors-canal
 - Avec le parent et les resolvers préconfigurés
- Le parent a besoin de vérifier de nouveau votre identité
- Comment protéger les délégations des enfants
 - Non sécurisées?
- Il y aura une période où la clé volée peut être utilisée pour générer des données sécurisées
 - Il n'y a pas de mécanisme de révocation de clé
- Une procédure d'urgence doit être en place



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**
- 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 ??**



Quelques Hics avec

DNSSEC

- 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 resolvers peuvent avoir des soucis avec le bit AD
 - **Faire mettre le bit AD dans les requêtes pour signaler l'état des resolvers ?**

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>

Tunisie-2015

Track SS-F : Services Internets évolutifs



AFRICA
INTERNET
SUMMIT'15
24 May to 5 June - Tunisia

AfNOG

Questions?

