Domain Name System

Extensions Sécurité

2 juin 2006

France Telecom R&D

Daniel Migault, Bogdan Marinoiu
mglt.biz@gmail.com, bogdan.marinoiu@polytechnique.org

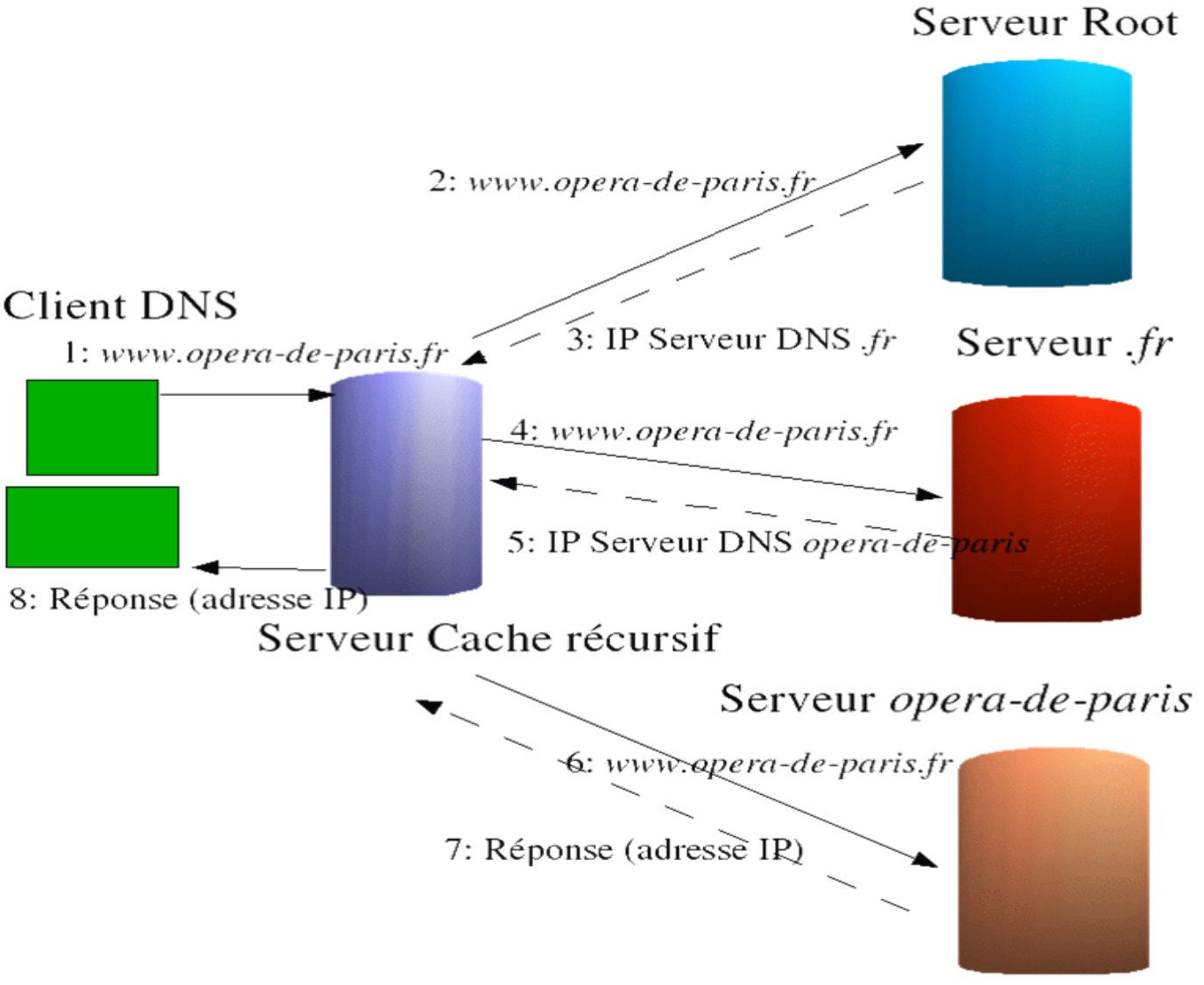
Introduction Extentions de Sécurité DNS

- Problématique :
  - Qu'est-ce que le système DNS?
  - Pourquoi sécuriser DNS?
  - Comment sécuriser DNS?
- Structure :
  - Rappel sur DNS et l'absence de sécurité
  - Rappel sur DNSSEC / IPsec
  - Description et analyse des tests

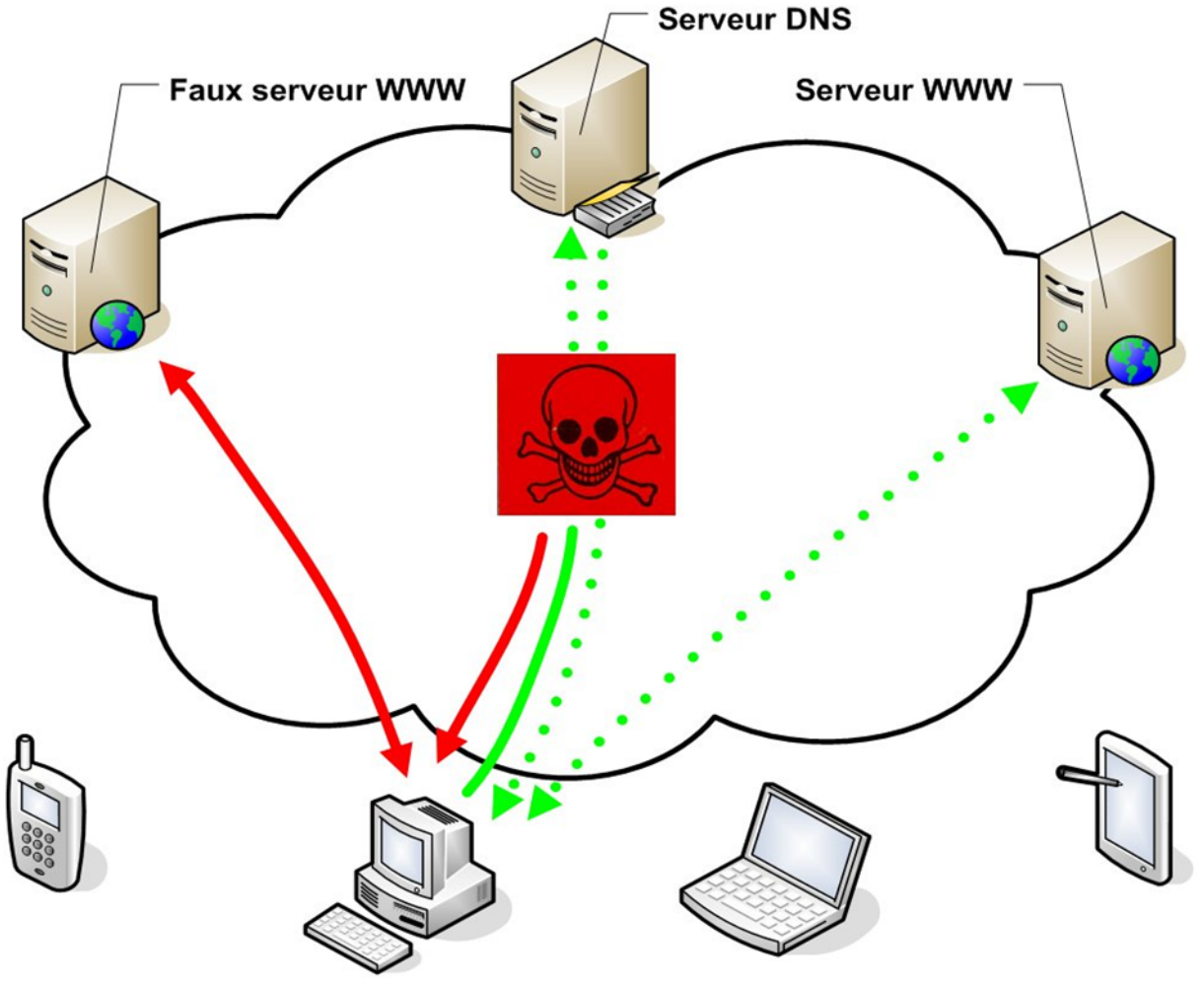
DNS Le système de nommage

- Le système DNS[1] est un protocole et une architecture permettant d'établir un lien entre un nom de domaine et une adresse IP. Le protocole est définit par l'IETF[2]
- Ce système est de plus en plus utilisé pour héberger d'autres fonctions nécessitant des mises à jour fréquentes, de permettre l'administration des données par de nombreux utilisateurs.
- Ce système est au cœur d'un certain nombre d'attaques comme les attaques de type "Poisonning"[3], "Spoofing"[4], "Denial of Service" (DoS)[5], "Phishing"[6] / "Pharming"[7], "Tracing"[8], et "Man-in-the-Middle" (MiM)[9]...
- Les mécanismes de sécurité considérés dans la présentation sont IPsec et DNSSEC.

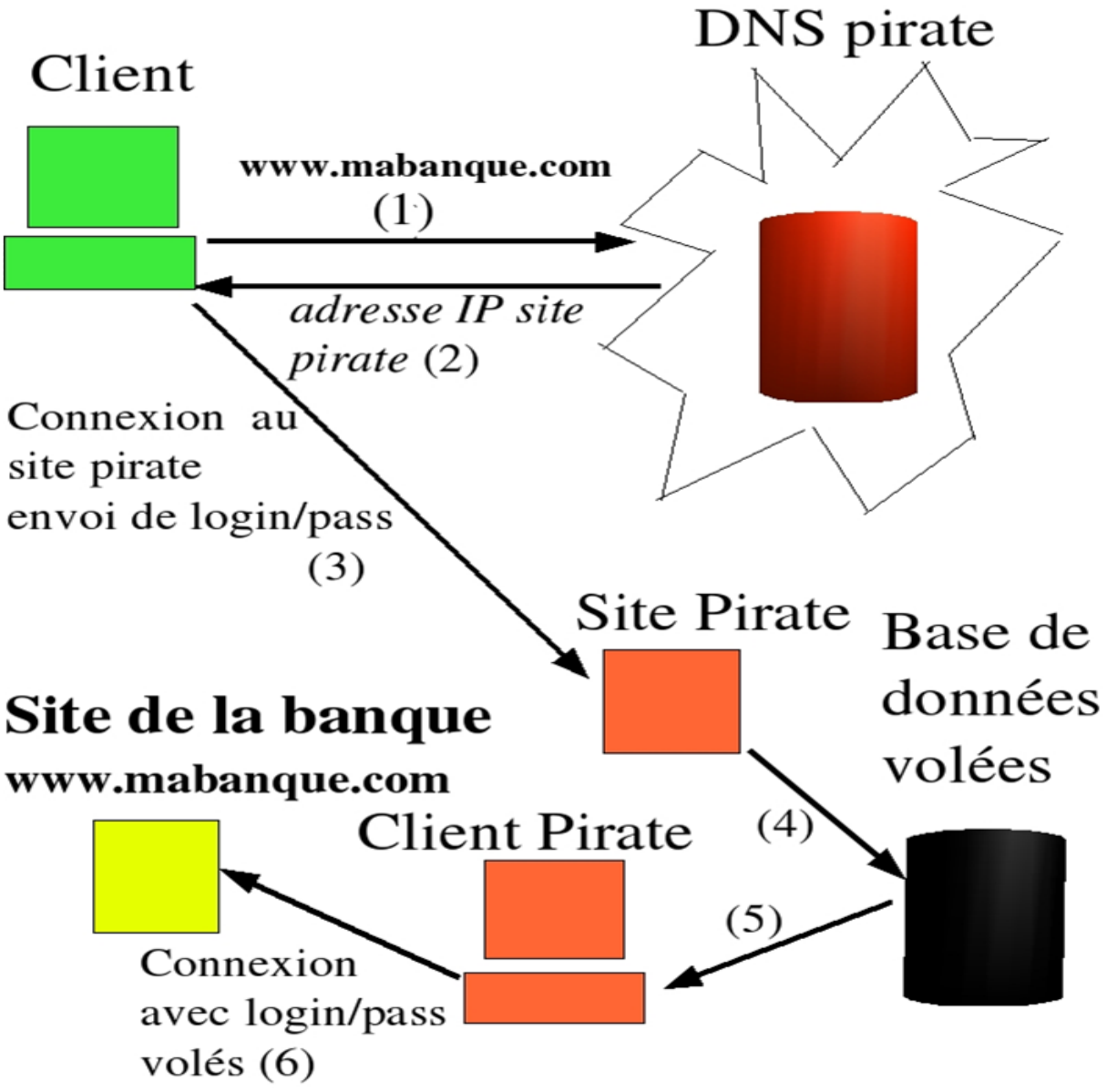
DNS Résolution d'un nom de domaine



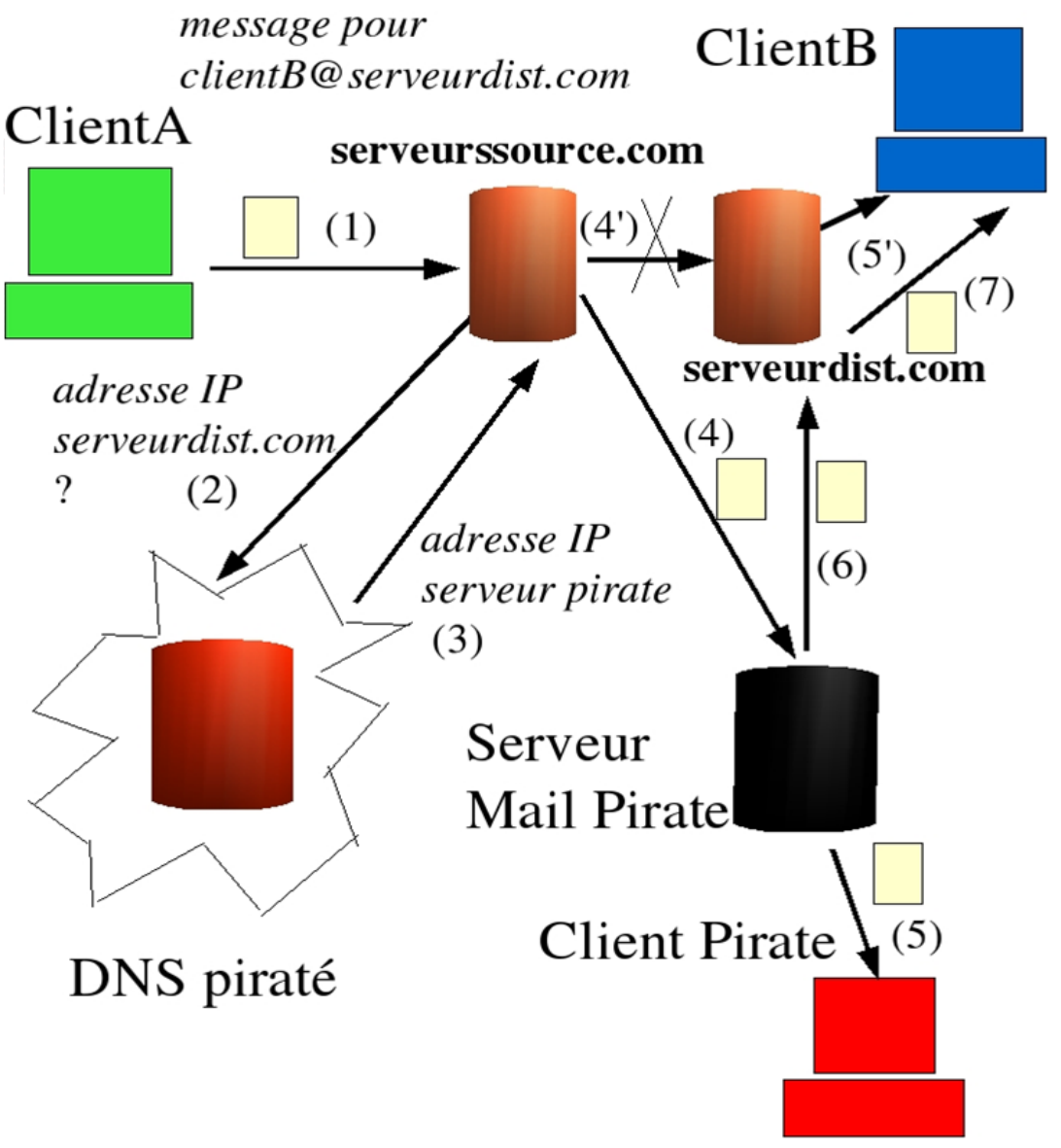
DNS Exemple d'attaque (MiM)



DNS Exemple d'attaque (Pharming)



DNS Exemple d'attaque (Tracing)



DNSSEC DNS Security Extention[10]

Standardisée par l'IETF, DNSSEC sécurise le DNS sur deux niveaux, à l'aide la cryptographie symétrique :

- Local
  - Clef de zone ZSK[11] (type DNSKEY)
  - Signatures des enregistrements (type RRSIG)
  - Pointeur vers l'enregistrement suivant (type NSEC)
- Global (Chaîne de confiance)
  - Clef d'identification KSK[12]
  - Signature de délégation DS[13]

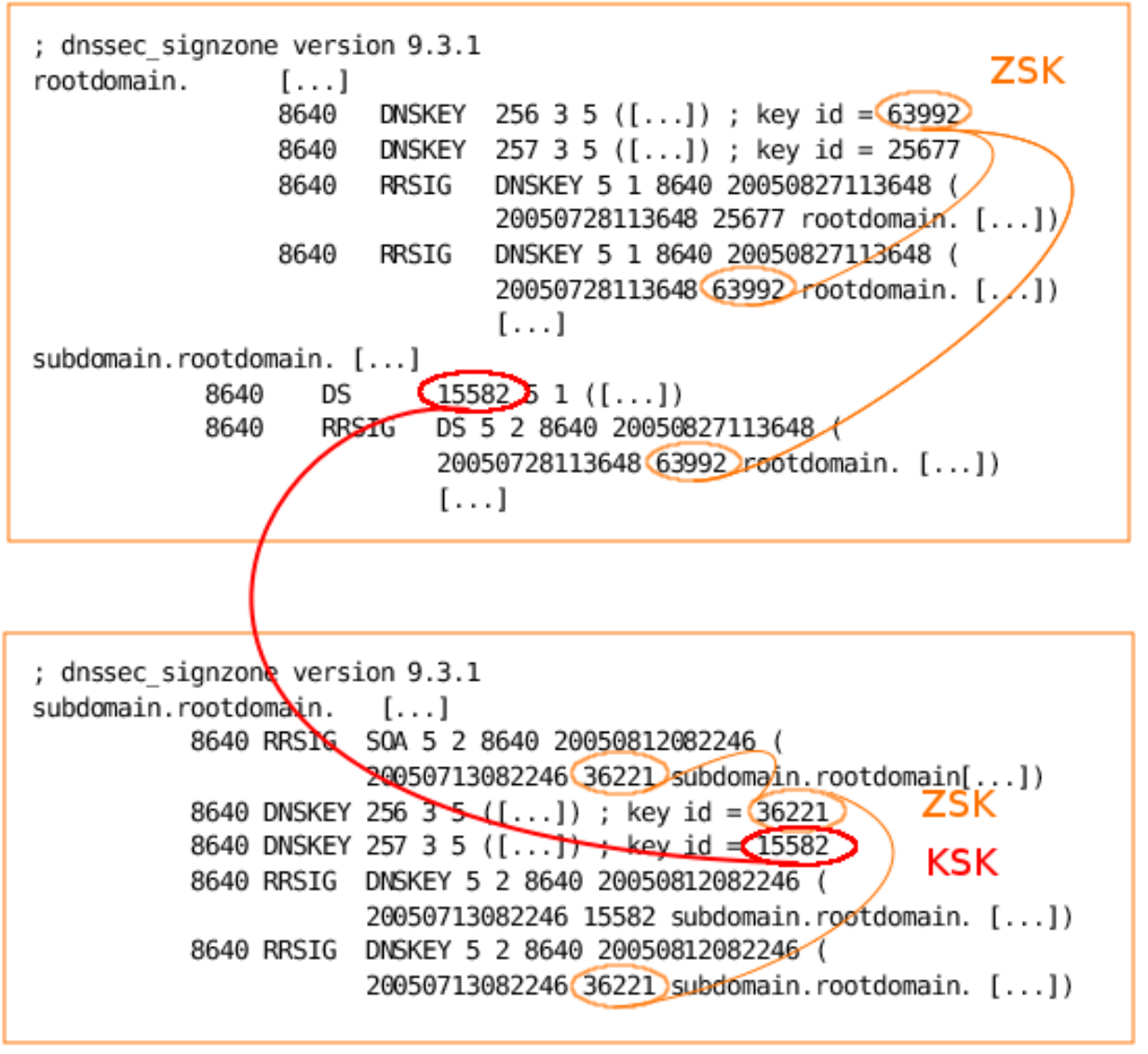
Description d'une zone Fichier DNS

```
rootdomain.       8640    IN SOA  dnssec1.rootdomain. mglt\.biz.gmail.com(
                                  2005070601; serial
                                  10000 ; refresh (2 h 46 min 40 s)
                                  20000 ; retry (5 h 33 min 20 s)
                                  604800 ; expire (1 week)
                                  10000 ; minimum (2 h 46 min 40 s)
                  8640    NS      dnssec1.rootdomain.

dnssec1.rootdomain.
              8640 IN   AAAA    2001:688:1f8b:1d5a:250:4ff:febe:12fa

dnssec2.rootdomain.
                        [...]
```

Sécurité Locale RRSIG, ZSK, NSEC

```
; dnssec_signzone version 9.3.1
rootdomain.       8640    IN SOA   dnssec1.rootdomain. mglt\.biz.gmail.com(
                                   2005070601 10000 20000 604800 10000 )
                  8640    RRSIG    SOA 5 1 8640 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])
                  8640    NS       dnssec1.rootdomain.
                  8640    RRSIG    NS 5 1 8640 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])
                 10000    NSEC     dnssec1.rootdomain. NS SOA RRSIG
                                   NSEC DNSKEY
                 10000    RRSIG    NSEC 5 1 10000 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])
                  8640    DNSKEY   256 3 5 ([...]) ; key id = 63992
                  8640    DNSKEY   257 3 5 ([...]) ; key id = 25677
                  8640    RRSIG    DNSKEY 5 1 8640 20050827113648 (
                                   20050728113648 25677 rootdomain. [...])
                  8640    RRSIG    DNSKEY 5 1 8640 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])

dnssec1.rootdomain.
                  8640 IN AAAA     2001:688:1f8b:1d5a:250:4ff:febe:12fa
                  8640    RRSIG    AAAA 5 2 8640 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])
                  10000   NSEC     dnssec2.rootdomain. AAAA RRSIG NSEC
                  10000   RRSIG    NSEC 5 2 10000 20050827113648 (
                                   20050728113648 63992 rootdomain. [...])
dnssec2.rootdomain.
                          [...]
```

Sécurité Globale DS, KSK

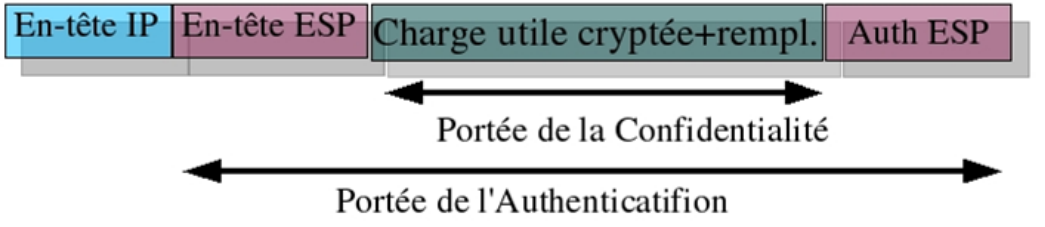


IPsec Security Architecture for the Internet Protocol

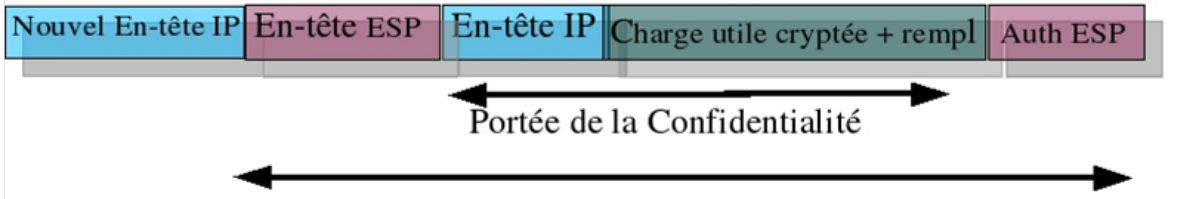
Le protocole **AH** en mode *transport*

Le protocole **AH** en mode *tunnel*

Le protocole **ESP** en mode *transport*



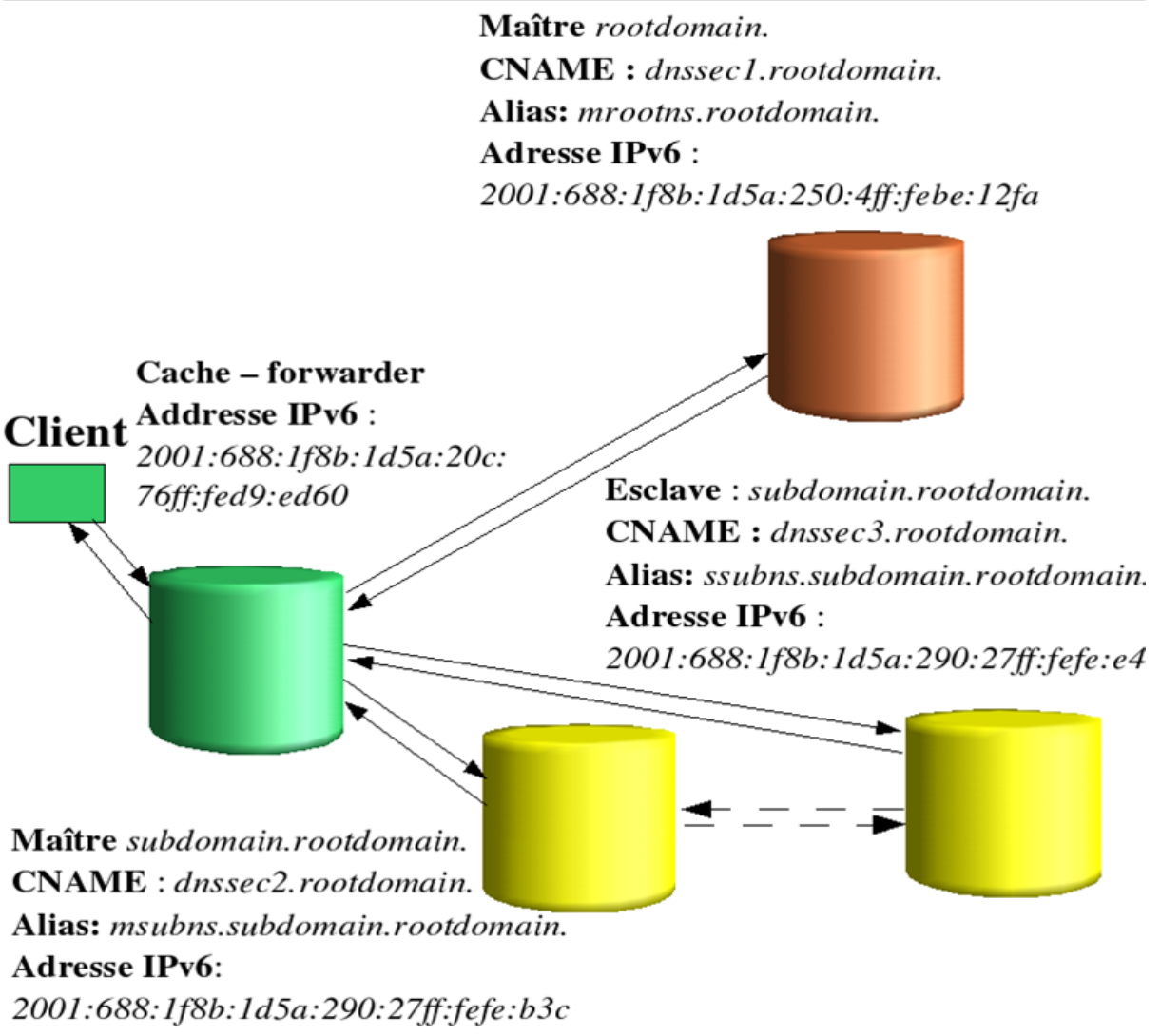
Le protocole **ESP** en mode *tunnel*



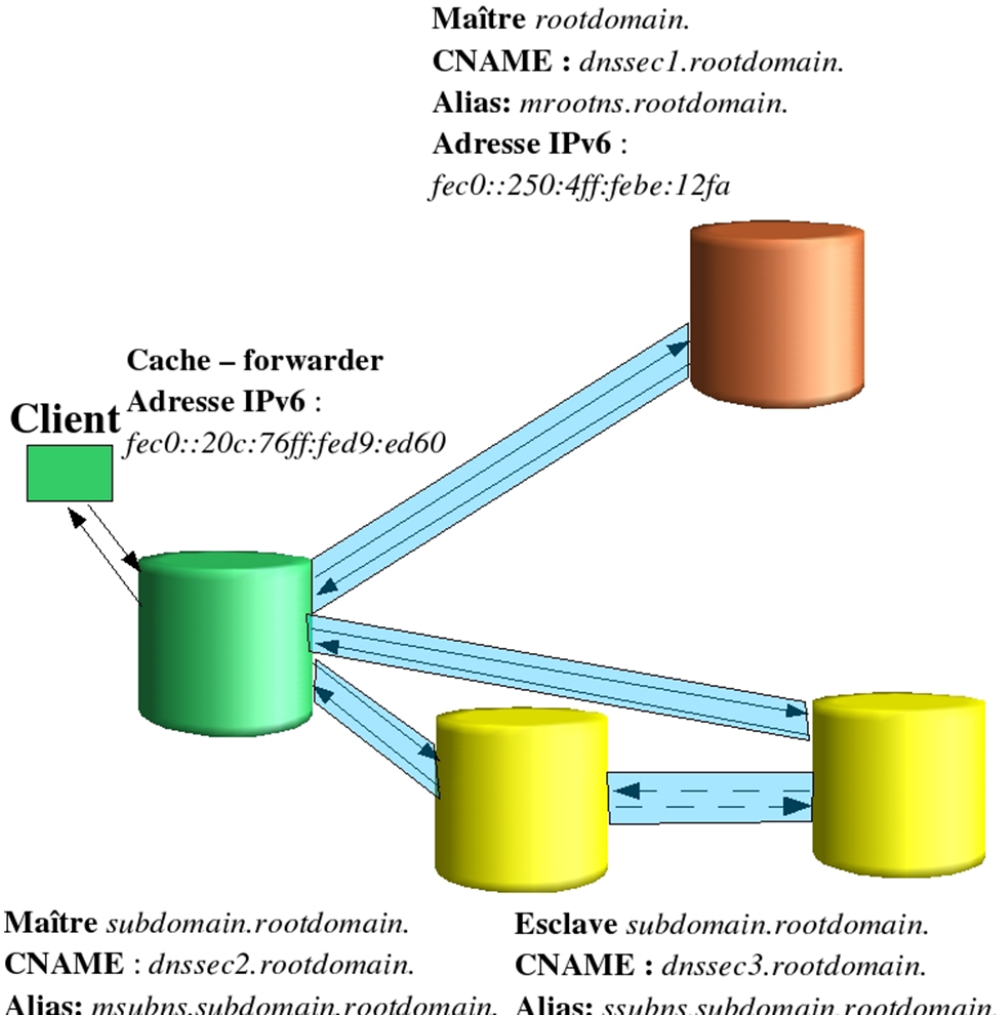
DNSSEC/IPsec Différence?

- IPsec :
  - Sécurise la couche de transport
  - Utilise la cryptographie symétrique
- DNSSEC :
  - Sécurise au niveau des données
  - Utilise la cryptographie assymétrique

Maquette de tests Architecture DNS



Maquette de tests Liens IPsec



Description Configurations et Paramètres

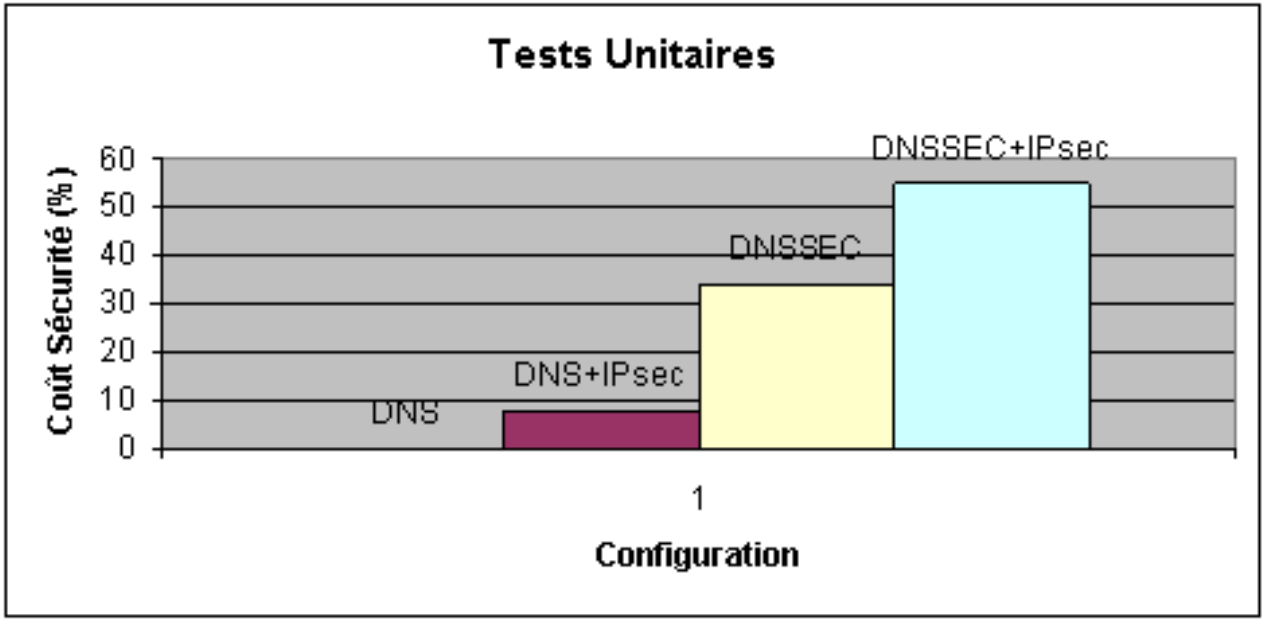
- Configurations testées :
  - DNS (référence)
  - DNS + IPsec (tunnels IPsec entre serveurs et le resolveur)
  - DNSSEC
  - DNSSEC + IPsec
  - TSIG (dans un seul test)
- Paramètres testés :
  - Temps de réponse à des requêtes
  - Occupation CPU / mémoire par le processus DNS
  - Temps de mises à jour des zones DNS

Description Nature des tests

- Natures de tests:
  - Tests unitaires (un seul client)
  - Tests en charge (plusieurs clients "simulés")
  - Tests de mise à jour
- Environnements testés:
  - Monoserveur : un serveur seul
  - Plateforme : l'ensemble de l'architecture DNS

Tests unitaires Temps de réponse

- Mesure du temps de réponse



- $\mathrm{DNS} < (\mathrm{DNS} + \mathrm{IPsec}) < \mathrm{DNSSEC} \ll (\mathrm{DNSSEC} + \mathrm{IPsec})$

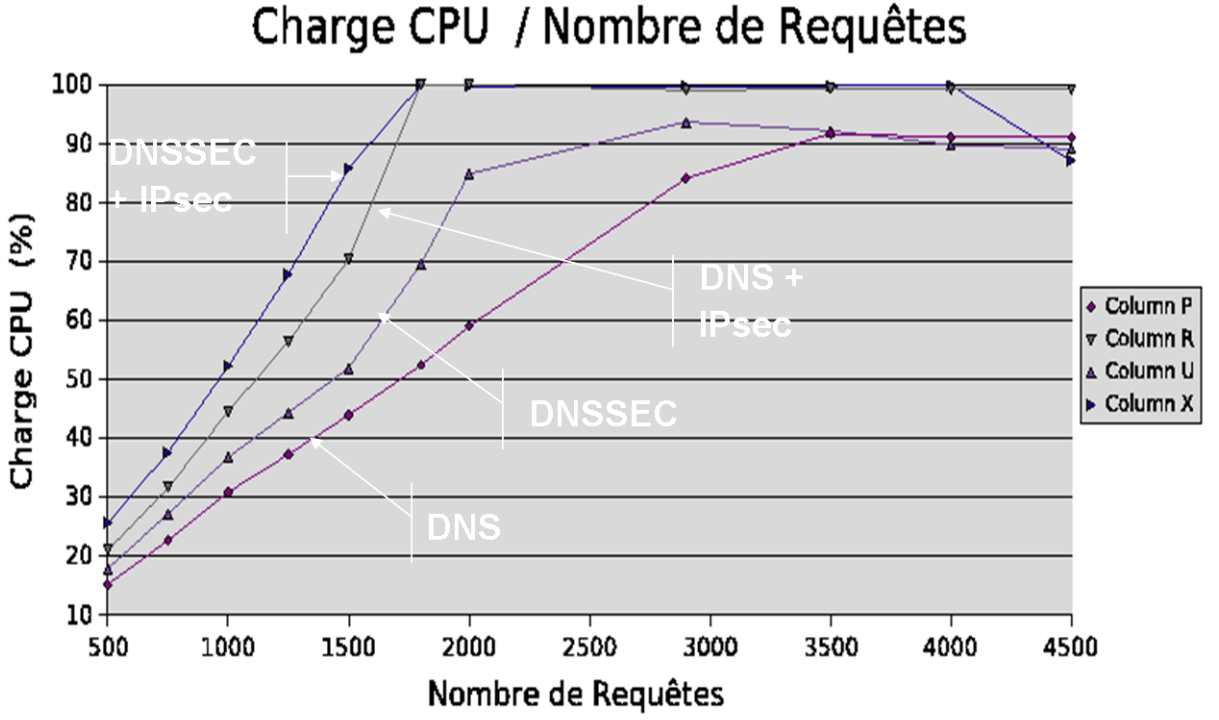
Tests unitaires Conclusion

- IPsec :
  - Peu gourmand en ressources (CPU, mémoire)
  - Plus rapide (une fois les tunnels installés)
- DNSSEC (plus de ressources nécessaires) :
  - Calculs de vérification sur le cache-forwarder/resolveur
  - Stockage d'enregistrements SIG, NSEC, DNSKEY etc...

Tests en charge Serveur Description

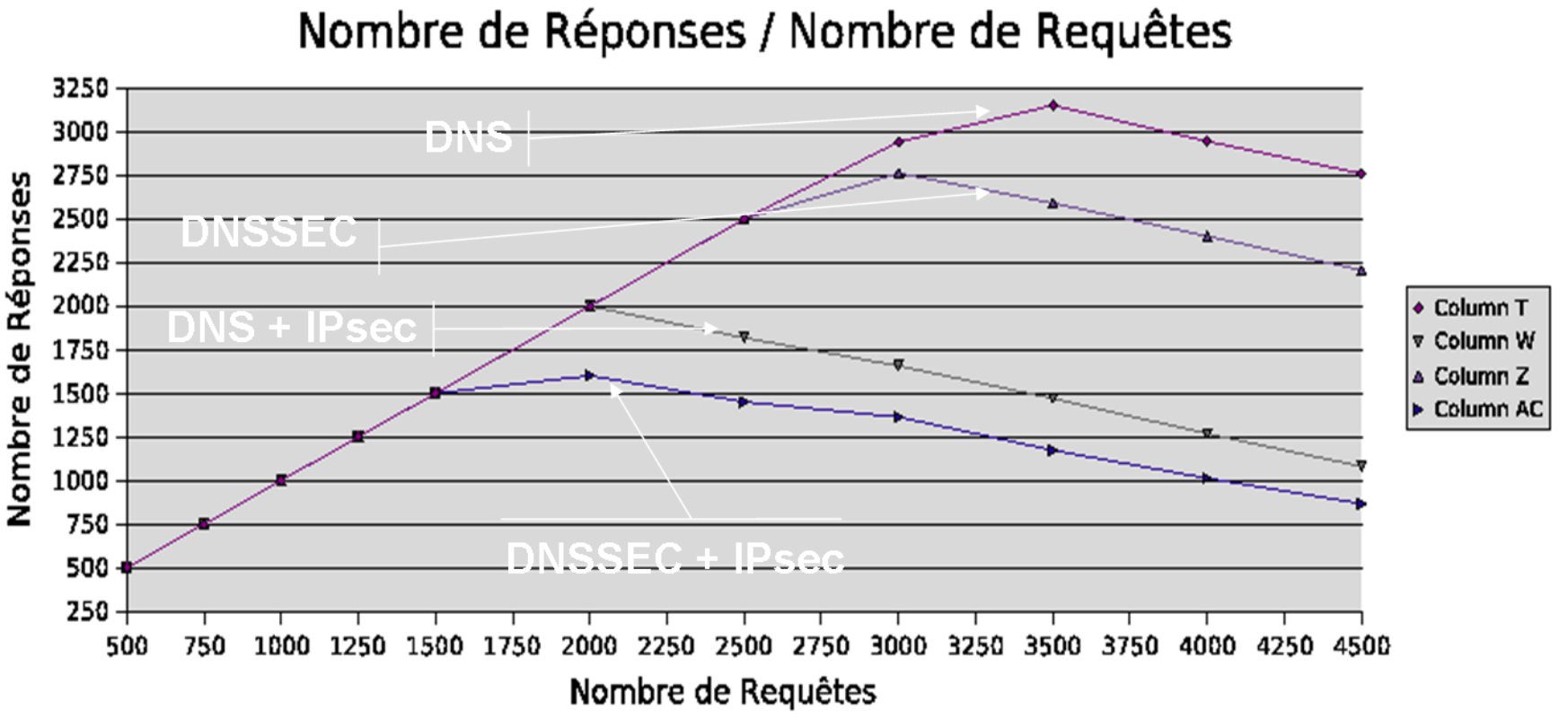
- Etude des propriétés des serveurs en régime de surcharge
- Simulation de plusieurs clients DNS non synchronisés
- Tests monoserveur / Plateforme
- Client Java à deux threads :
  - Un thread génère un nombre variable de requêtes
  - Un thread interprète les réponses

Tests en charge Serveur Point de rupture Machine



- Capacité maximale du serveur : Point de rupture machine : 100% (IPsec) / 90% (autres)
- $\mathrm{DNS} < \mathrm{DNSSEC} < \mathrm{DNS} + \mathrm{IPsec} < (\mathrm{DNSSEC} + \mathrm{IPsec})$

Tests en charge Serveur Point de rupture Service



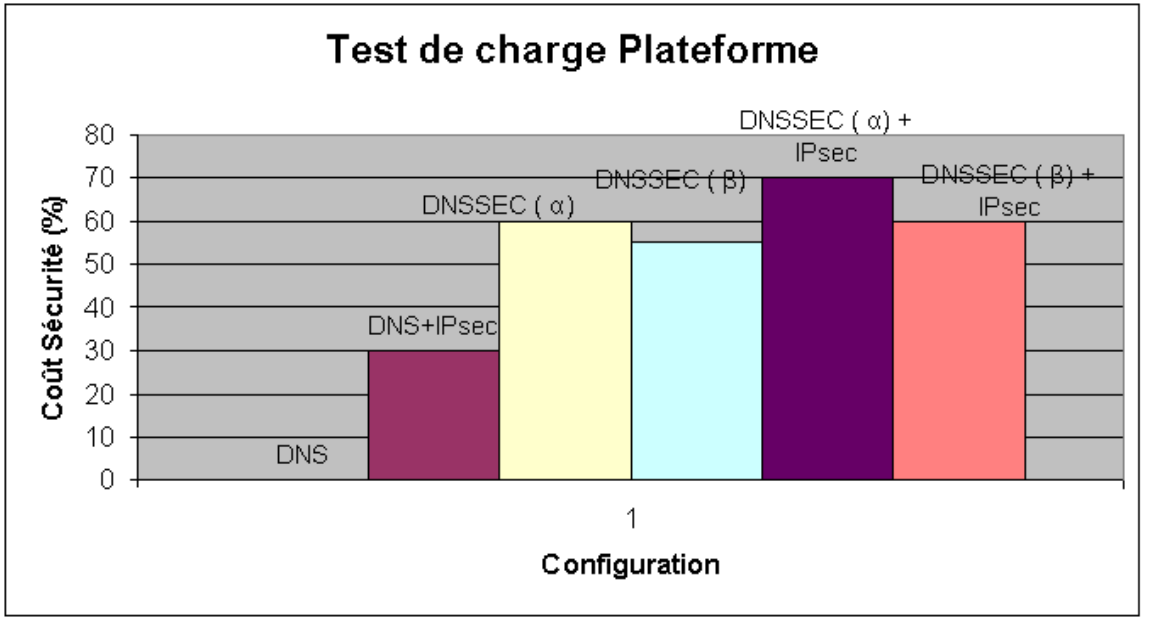
- Capacité maximale du service DNS : Point de rupture service (certaines requêtes sont "ignorées")
- $\mathrm{DNS} < \mathrm{DNSSEC} < \mathrm{DNS} + \mathrm{IPsec} < (\mathrm{DNSSEC} + \mathrm{IPsec})$

Tests en charge Plateforme Description

- Utilisation d'un relais (resolveur / cache forwarder).
- DNSSEC ou (DNSSEC + IPsec) avec ou sans vérification de signature (CD=0/1)
- 6 configurations de tests possibles :
- Une requête, 3 résultats possibles :
  - Réponse correcte : NO ERROR
  - Déni de service (surcharge) : SERVFAIL
  - Rejet de la requête (surcharge) $\Rightarrow$ pas de réponse

Tests en charge Plateforme Résultats

- Capacité maximale de traitement de requêtes par une plateforme :



[a] avec vérification de signature

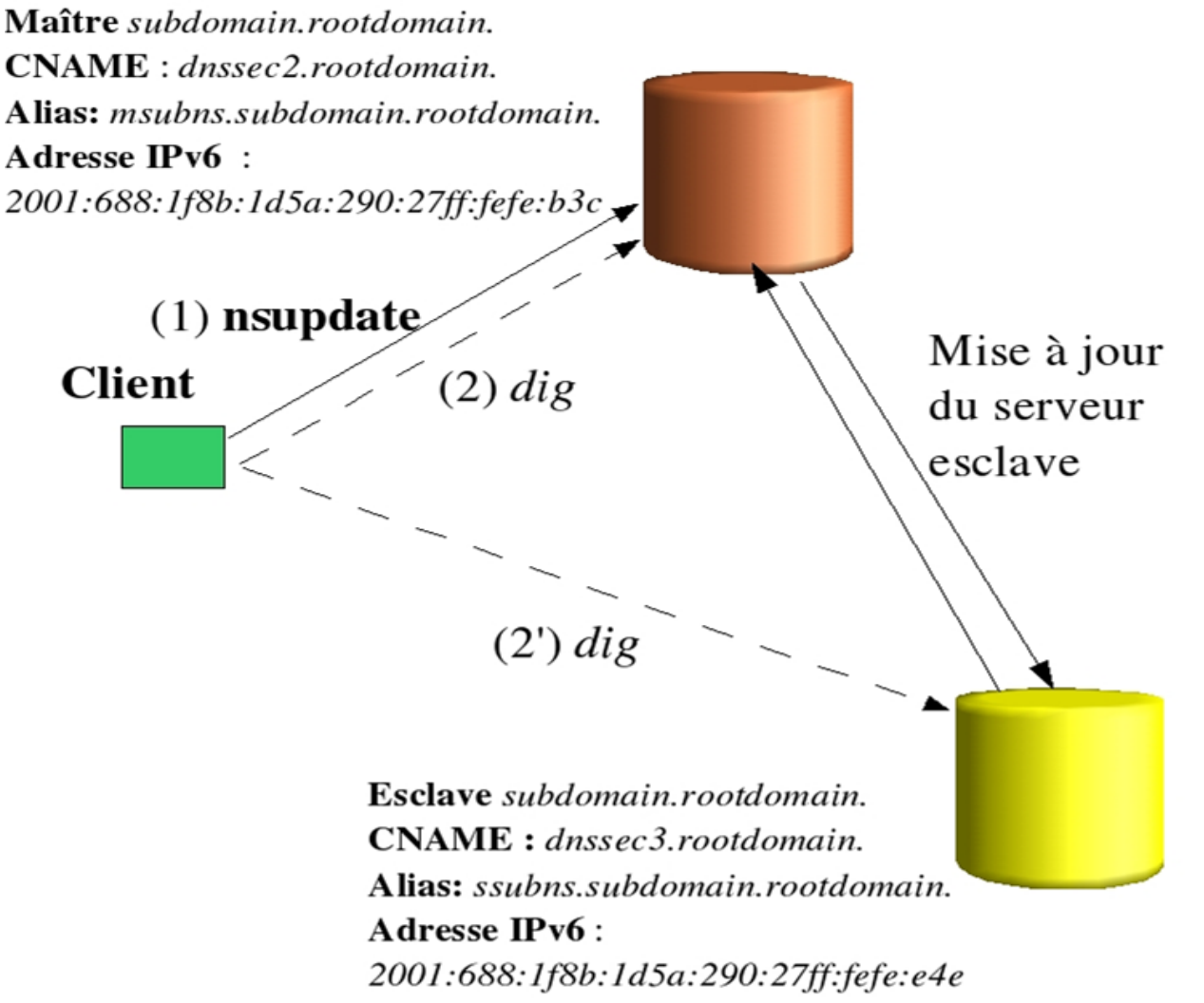
[b] sans vérification de signature

- DNS $<$ DNS $+$ IPsec $<$ DNSSEC $<$ (DNSSEC $+$ IPsec)

Tests en charge Plateforme Conclusion

- Les points de rupture service de la plateforme apparaissent pour des valeurs plus petites (par rapport aux valeurs pour les tests monoserveur).
- Les serveurs de la plateforme ne sont pas surchargés.
- Le relais est un "goulot d'étranglement". Il est le premier élément de l'architecture à devenir surchargé.

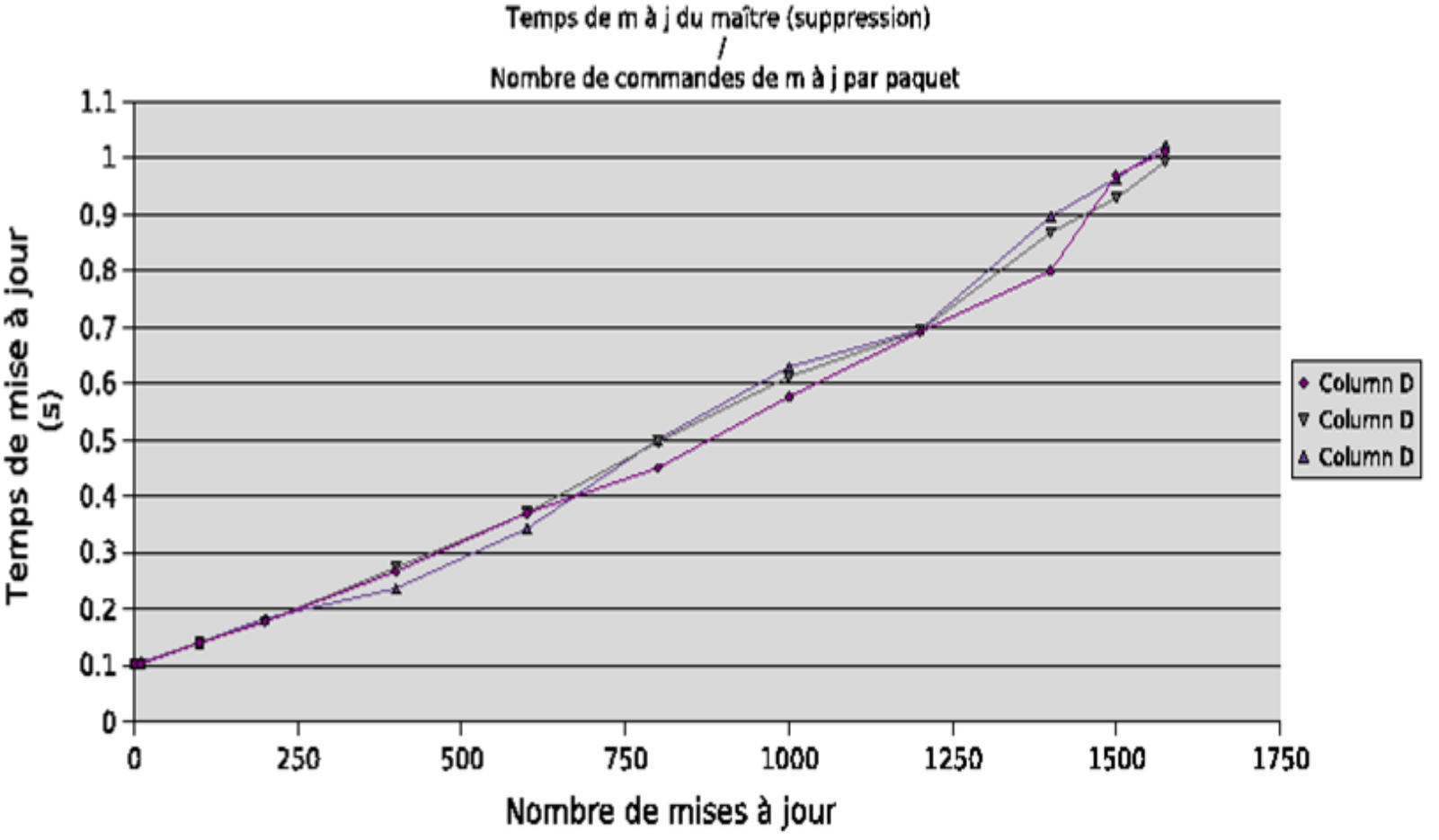
Mise à jour Description



- (1) m. à. j.
- (2) vérification (`dig`) sur le maître ou sur l'esclave

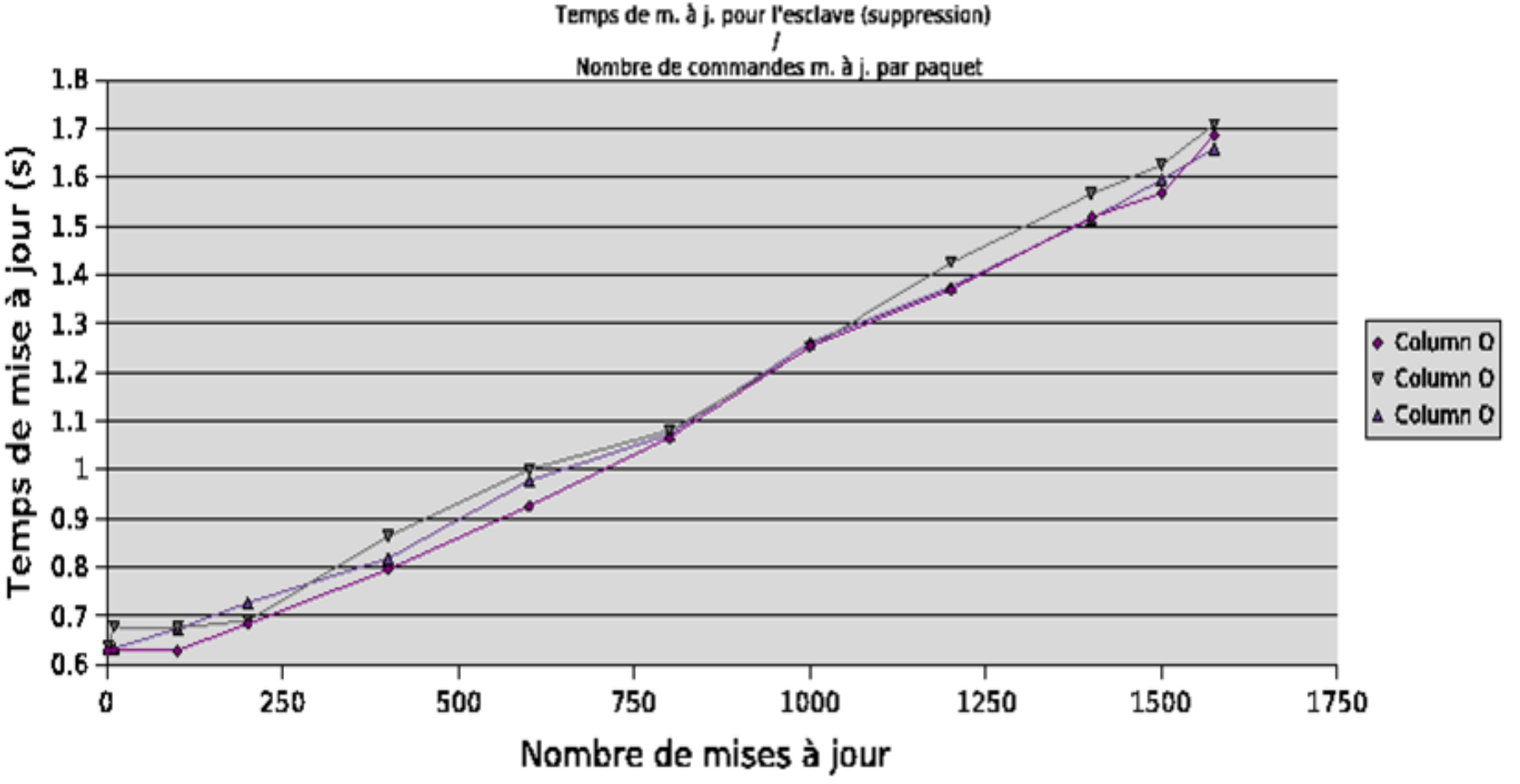
Mise à jour Suppression du Maître

- Configurations : DNS, (DNS + IPsec), TSIG



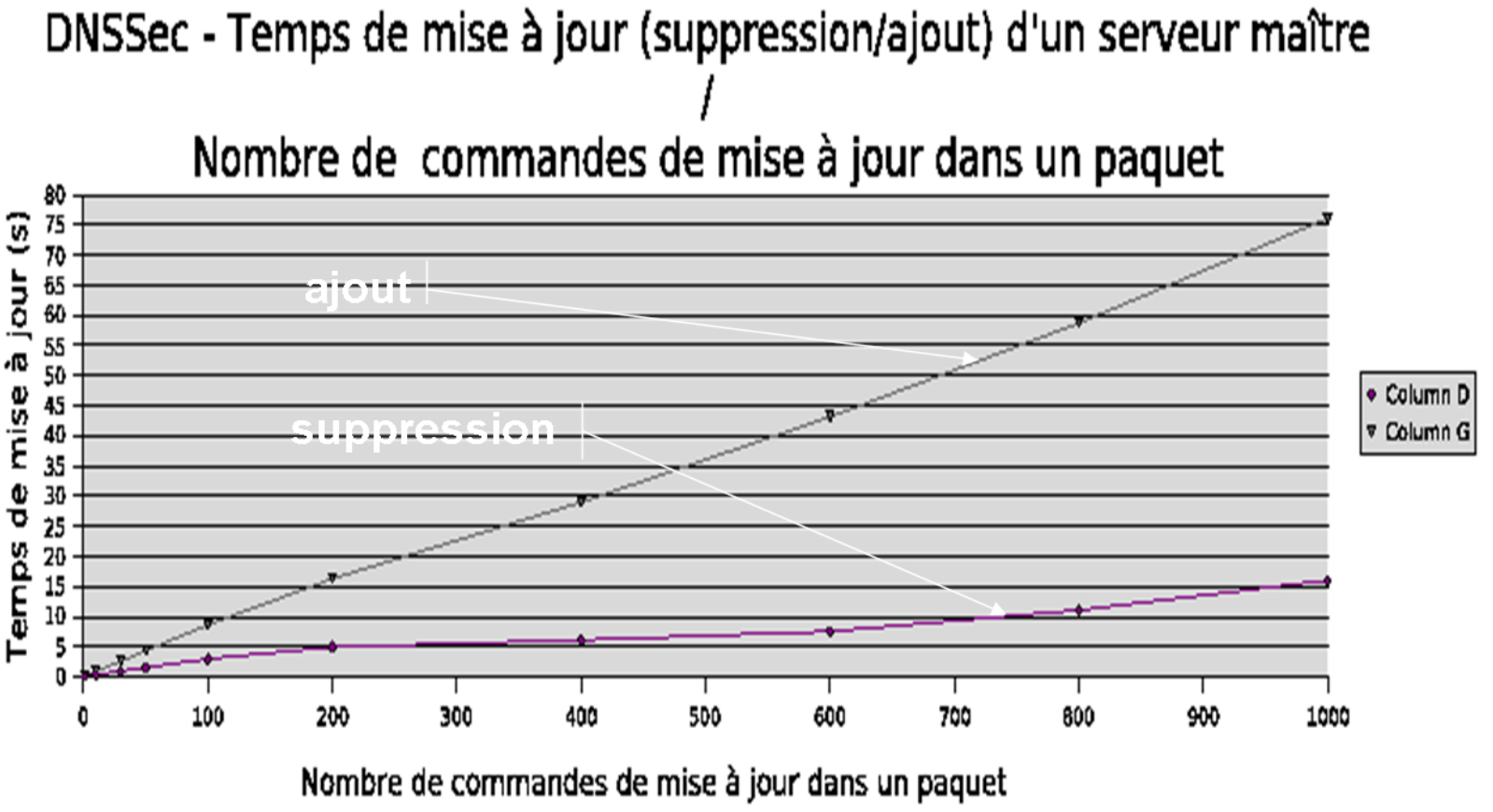
Mise à jour Suppression de l'esclave

- Configurations : DNS, (DNS + IPsec), TSIG



Mise à jour Ajout / Suppression avec DNSSEC

- Configuration : DNSSEC



Conclusion Les Résultats des tests

- Pas de solutions Miracle!!!
- Toujours considérer l'ensemble des éléments de l'architecture.
  - Sécuriser les données?
  - Sécuriser les couches de transport?
  - peut-on distribuer les clés?

Conclusion Les paramètres et protocoles

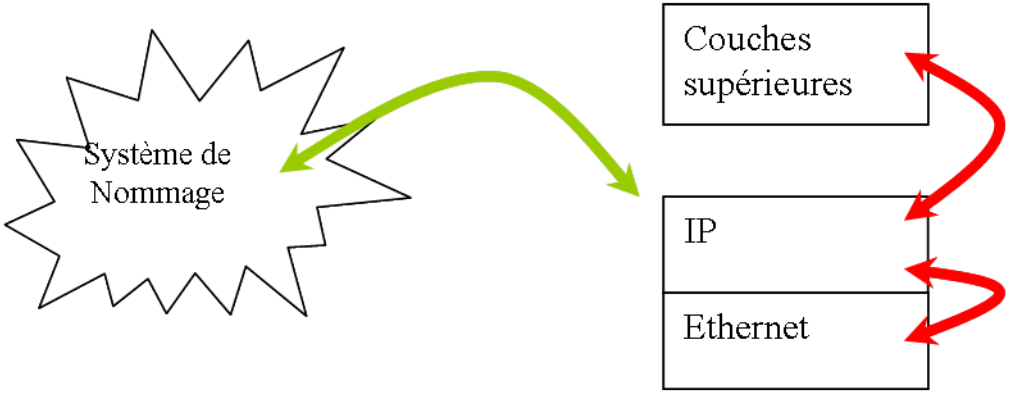
- Paramètres à considérer dans les tests :
  - Temps de réponse d'un serveur / plateforme
  - Capacité maximale de traitement d'un serveur / plateforme
  - Temps de mise à jour des serveurs
- Particularités des protocoles :
  - TSIG : peu coûteux (m. à. j.), authentification + intégrité, configuration manuelle lourde
  - IPsec : authentification + intégrité (+confidentialité?), configuration facile avec IKE, peu coûteux
  - DNSSEC : peu adapté pour les m. à. j. , authentification de la source de la donnée !!! + intégrité

Conclusion Les Résultats des tests

- Les principes à retenir :
  - Temps de réponse de la plateforme :
    - $(\text{DNS} + \text{IPsec})$ est plus appropriée que DNSSEC
  - Capacité de traitement des requêtes par un serveur de nom :
    - DNSSEC est plus appropriée que $(\text{DNS} + \text{IPsec})$
  - Capacité de traitement des requêtes par la plateforme :
    - $(\text{DNS} + \text{IPsec})$ est plus appropriée que DNSSEC

Conclusion Ouverture

- Après la sécurisation du lien adresse IP / nom de domaine (par DNSSEC), sécurisation du lien couche IP couche Ethernet ?
- Réponse possible : protocole SEND (SEcure Neighbour Discovery)



Notes

[1] DNS : Domain Name System

[2] IETF : The Internet Engineering Task Force (**http://www.ietf.org/**

[3] Poisioning : Attaque visant à polluer la cache d'un serveur DNS par des informations fausses

[4] Spoofing : attaques reposant sur l'usurpation d'identité.

[5] Denial of Service (DoS) : attaque visant à rendre une application informatique incapable de répondre aux requêtes

[6] Phishing : Attaque qui consiste à usurper l'adresse IP d'un site, de manière à ce que l'URL soit redirigée vers un autre site que le site désire (cf. DNS hijacking attack).

[7] Pharming : Attaque qui consiste à rediriger le client vers un site pirate qui est l'exacte copie du site souhaité.

[8] Tracing : Attaque permettant d'obtenir des informations confidentielles.

[9] Attaques Man-in-the-Middle : Attaque où l'attaquant est capable de lire, d'insérer et de modifier les messages chiffrés entre deux partis, sans que ni l'un ni l'autre ne puisse s'en douter.

[10] DNSSEC :RFC4033, RFC4034, RFC4035

[11] ZSK : Zone Signing Key

[12] KSK : Key Signing Key

[13] DS : Delegation Signer

[14] TKEY : RFC4301