Domain Name System : Attaques et sécurisation

Hamza HMAMA
Guillaume LUCAS

Faculté des Sciences et Techniques
Limoges

30 mai 2012

Introduction

- DNS comme projet
- Toute transaction en réseau commence par DNS
- DNS = Internet

1. DNS
   - Présentation
   - Mise en oeuvre
   - Faiblesses
2. DNSSEC
   - Présentation
   - Présentation détaillée
   - Faiblesses
3. Conclusion

Présentation DNS

- Nom de domaine : Identifiant unique pour un ensemble de machines
- Conception : dès 1982

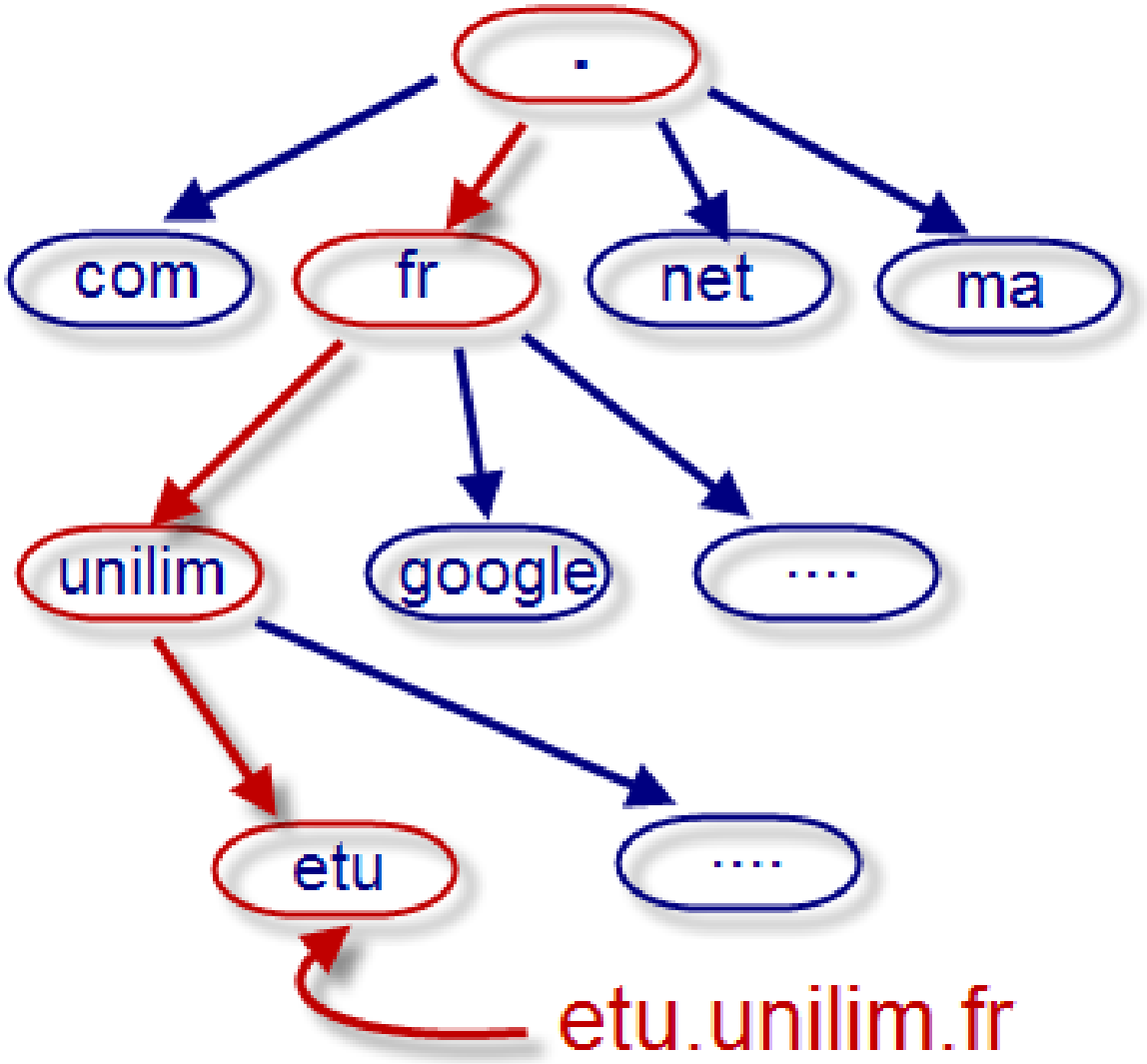
Services

- Enregistrement
- Résolution

Caractéristiques

- Hiérarchique (pas centralisé !)
- Redondant
- Distribué

hiérarchie



Résolution

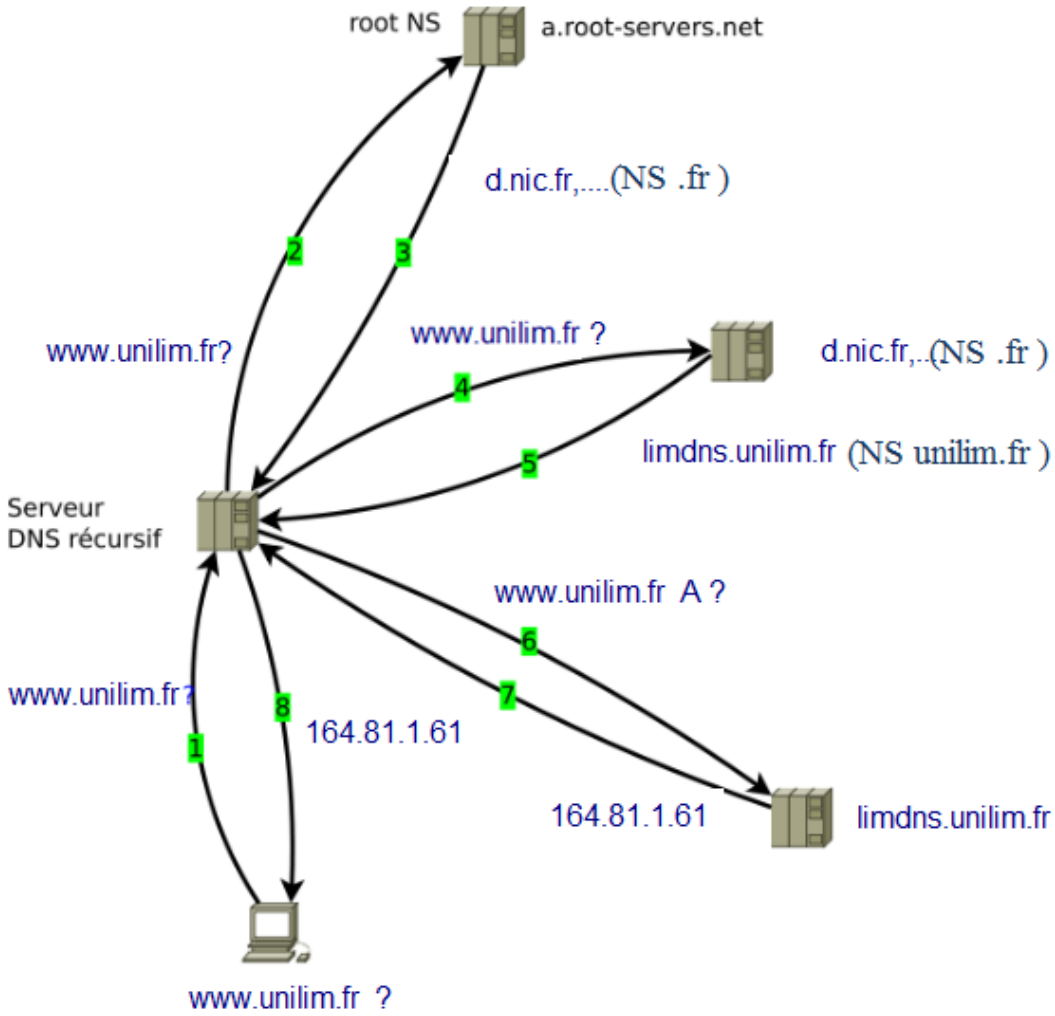
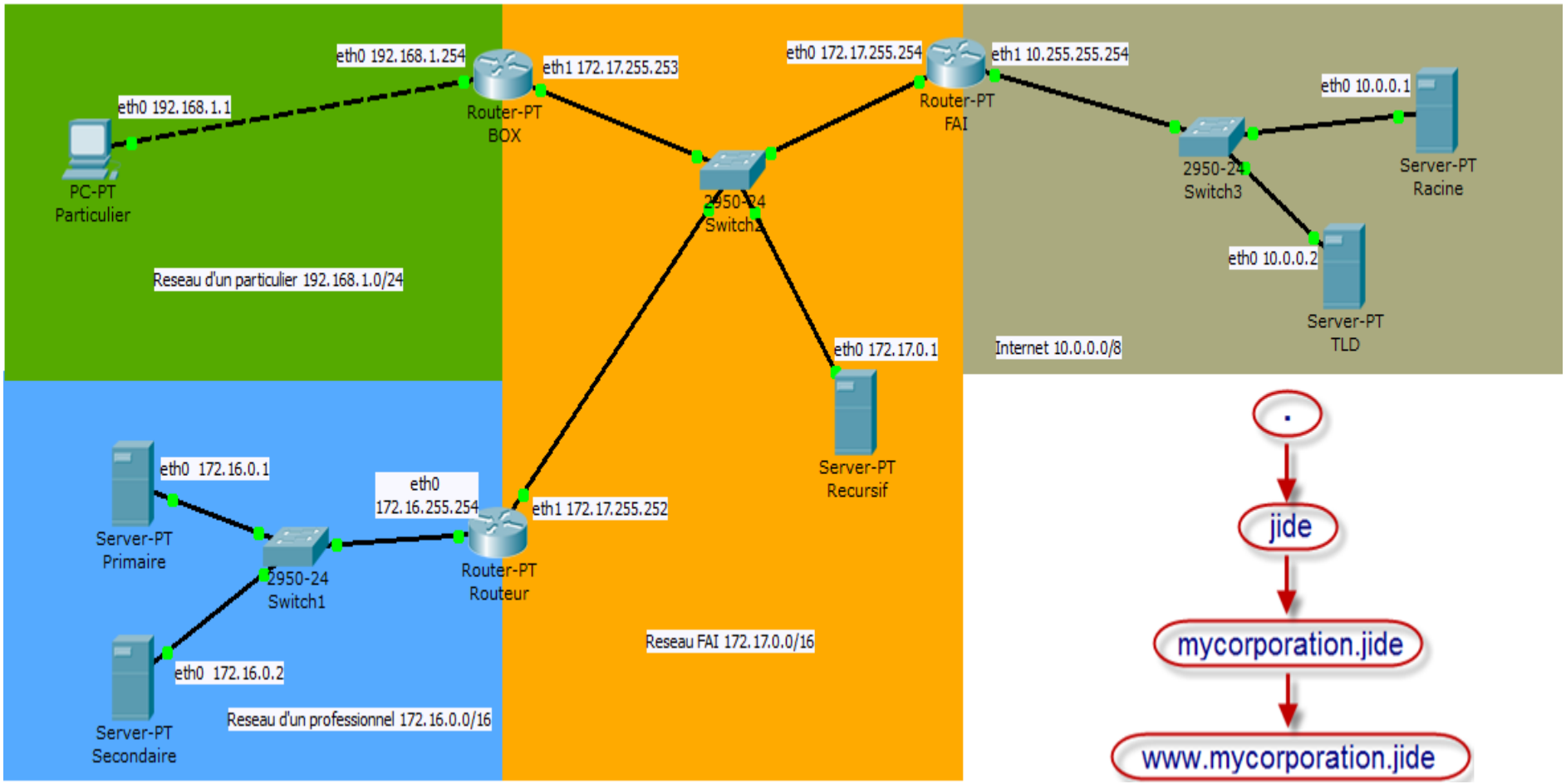


FIGURE: D'après : https ://fr.wikipedia.org/wiki/Fichier :DNS_iterations.svg.

Mise en oeuvre



Faiblesses

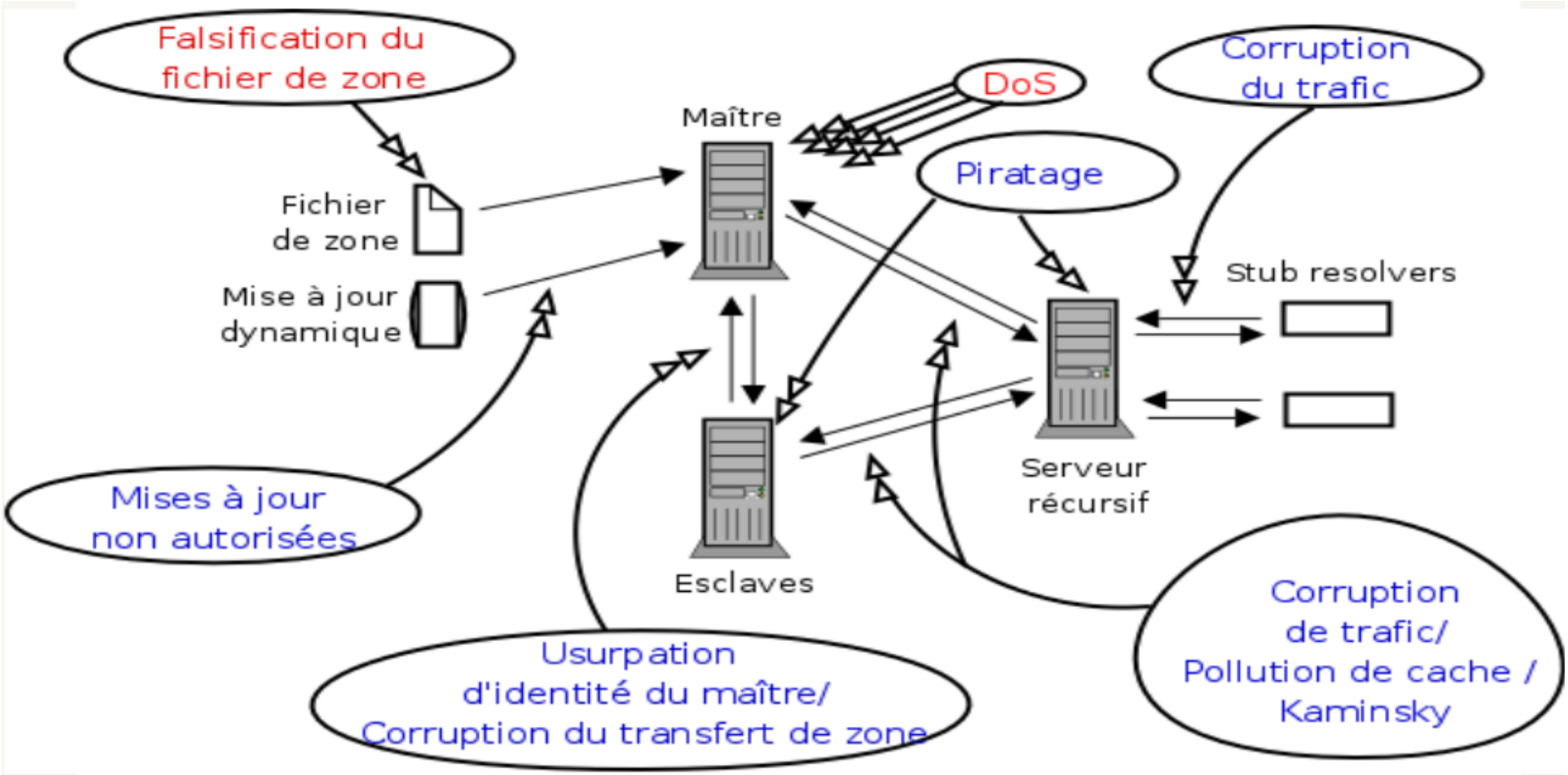


FIGURE: Source : présentation de Stéphane Bortzmeyer à SARSSI 2009.

Faiblesses

Mauvaise configuration

- Transfert de zone
- Serveur ouvert
- Serveur faisant autorité récursif

Ghost(busters)

- But : Maintien d'un nom domaine inexistant
- Intérêts : C&C, censure, ...

Amplification

- But : Provoquer un déni de service (DoS)
- Intérêts : Furtivité et efficacité

Faiblesses (Suite)

Empoisonnement de cache

- But : Introduire une réponse falsifiée
- Intérêt : Tromper les utilisateurs
- Impact limité

Kaminsky

- Optimisation de l'empoisonnement de cache
- Fort impact

DNSSEC

Apparition

- Mi-1990 : Réflexion sur les faiblesses de DNS
- 1999 : Émergence d'une première version
- 2001-2005 : Refonte

Extension

- Préserve le fonctionnement DNS
- Compatibilité

Objectif

- Authentifie les données uniquement
- Cryptographie asymétrique
- Évolutif

Présentation détaillée

Cryptographie

- Modèle à deux clés : KSK, ZSK
- Signature des données
- Roulement des clés

Nouveaux enregistrements

- RRSIG : stocke la signature
- NSEC : Non-existence
- NSEC3

- Problématique : Valider les signatures

Où trouver les clés ?

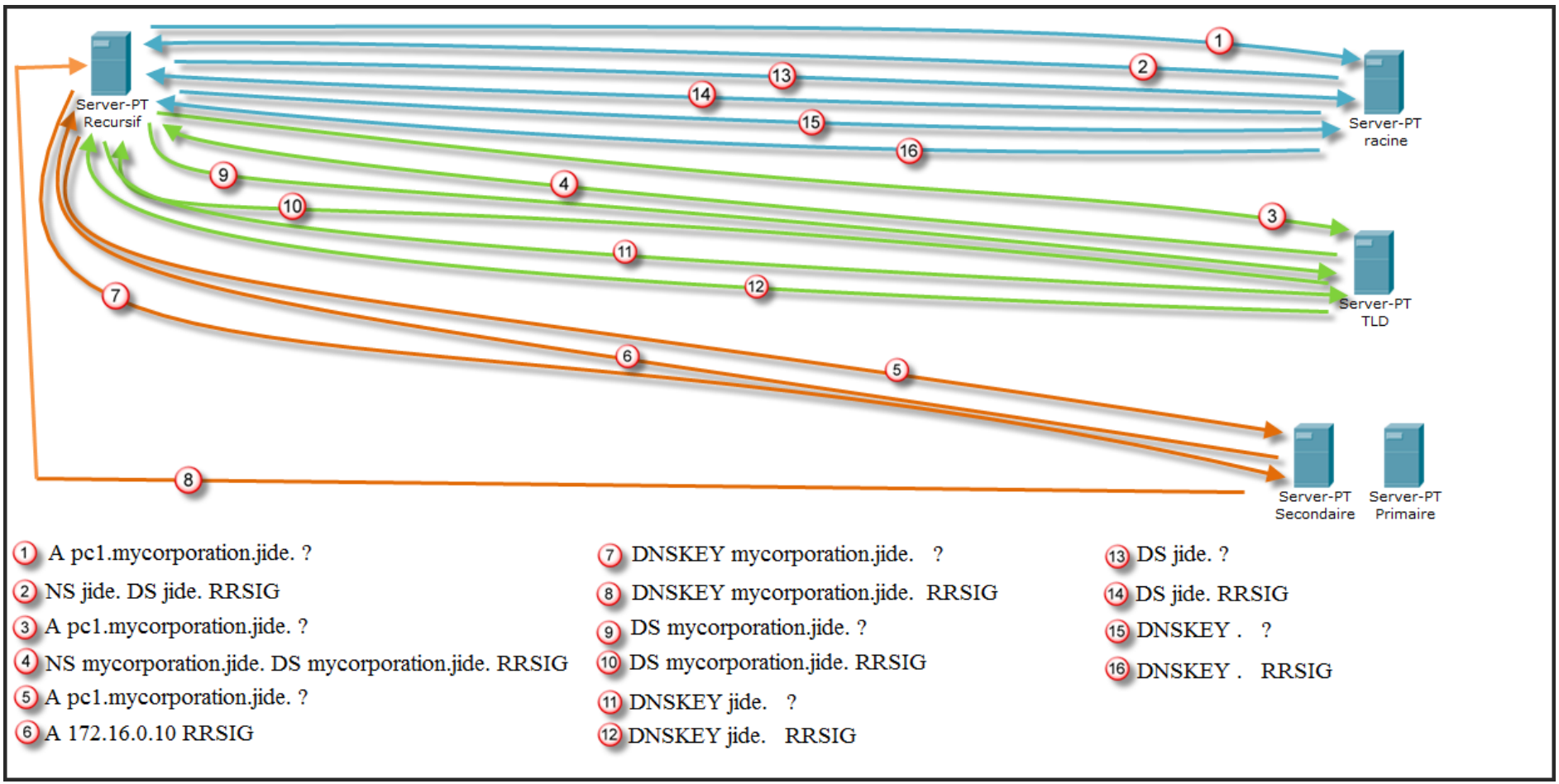
Solutions envisageables

- Historique : Distribuer les clés
- Regroupement des clés
- Diffuser les clés dans DNS

Chaîne de confiance

- Déléguer la confiance depuis un point
- Nouvel enregistrement : DS

Chaîne de confiance



Bilan des faiblesses

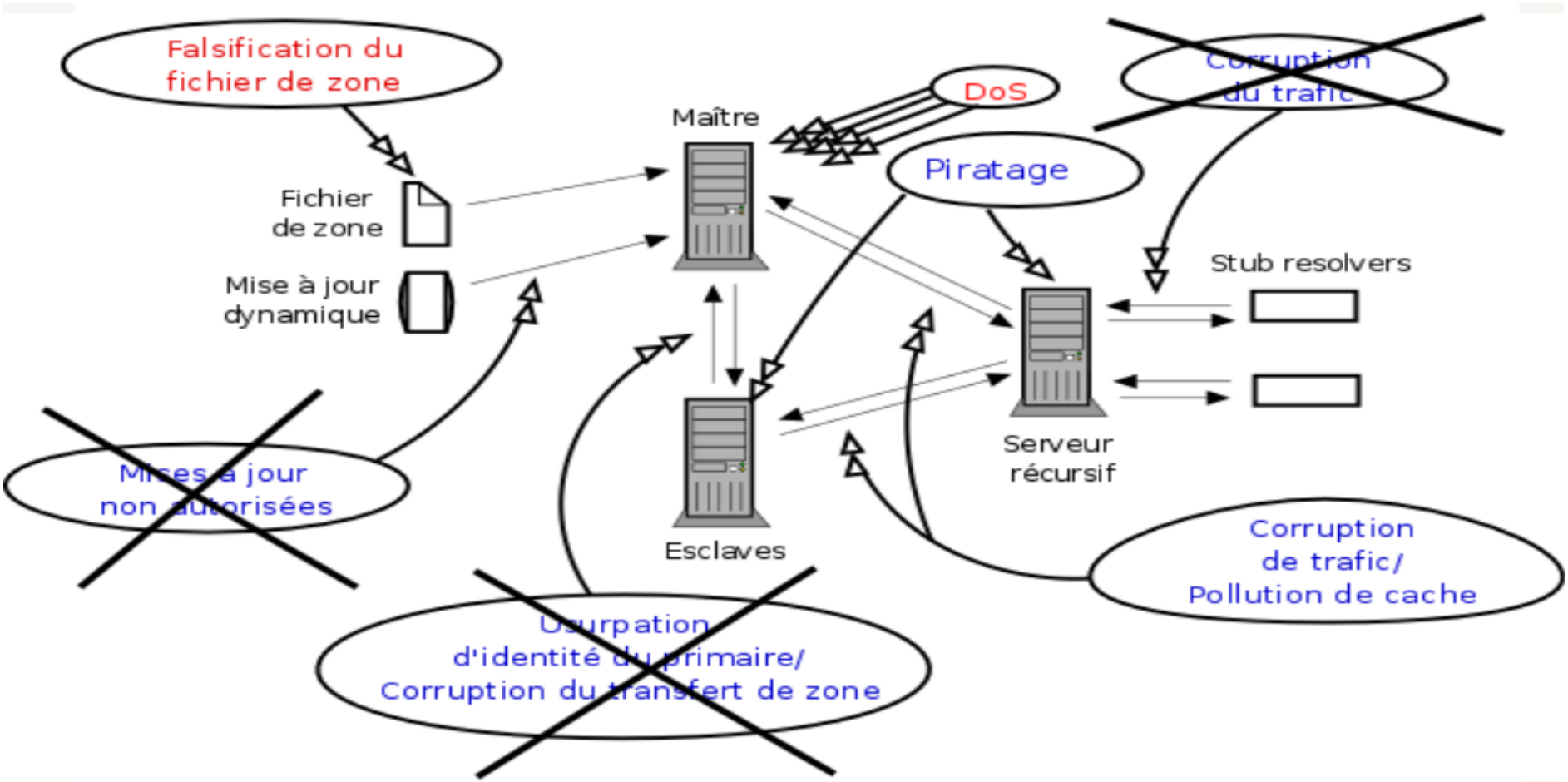


FIGURE: Source : présentation de Stéphane Bortzmeyer à SARSSI 2009.

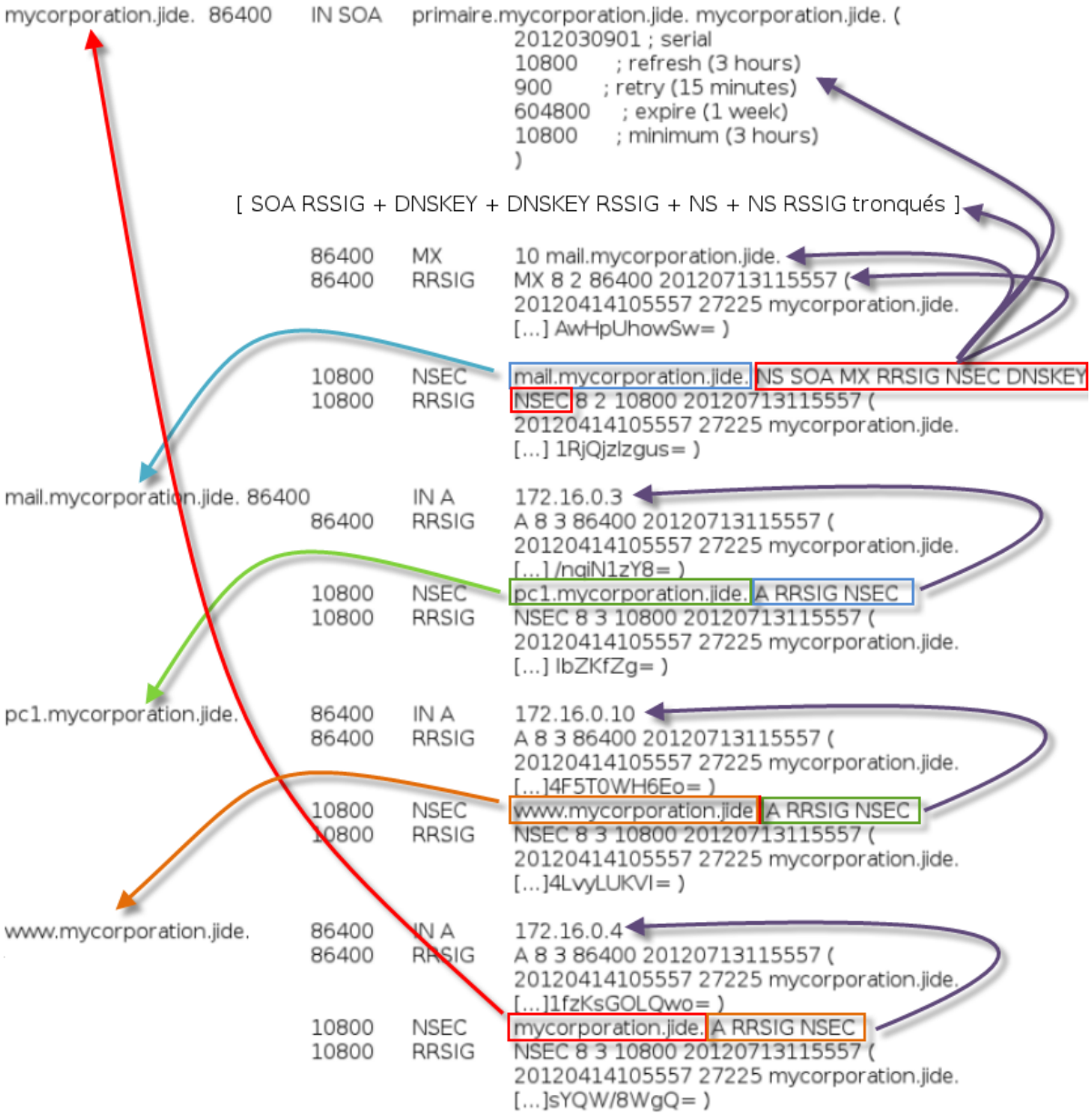
Faiblesses DNSSEC

- Mauvaise configuration toujours possible

Zone walking

- But : Obtenir tous les enregistrements d'une zone
- Intérêts :
  - Récupérer des informations sensibles
  - Compromettre un business-model

Zone walking (Demo)



Conclusion

Bilan DNS/DNSSEC

- DNS toujours utilisable
- DNSSEC solution efficace d'avenir ...
- ... mais à long terme

Bilan projet S6

- 2 maquettes réalisées
- Approfondir nos connaissances DNS
- Capables de mettre en place une technologie récente
- Gagner 2 (3 ?) kudos

Any Questions ? ?

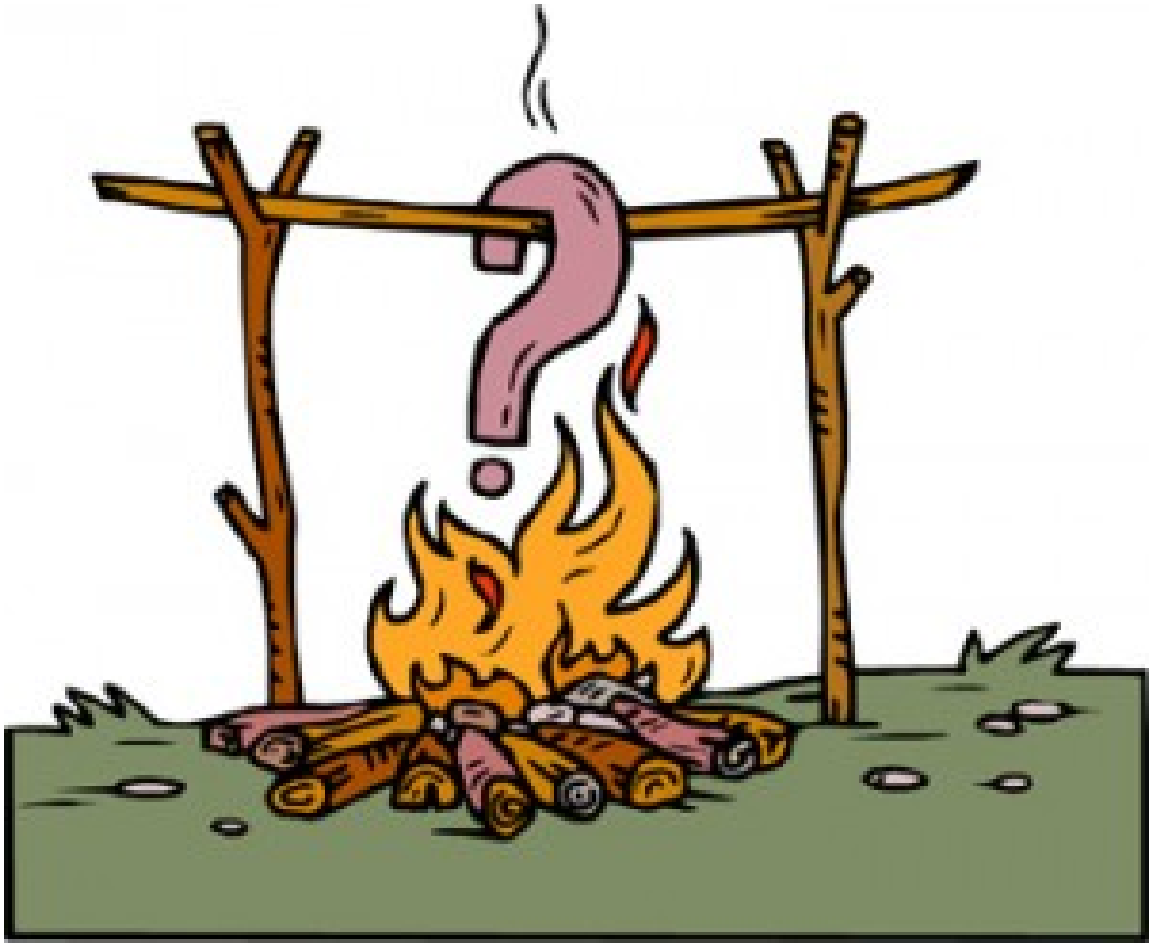


FIGURE: Source :
https ://somkritya.files.wordpress.com/2012/01/burning-question.jpg.