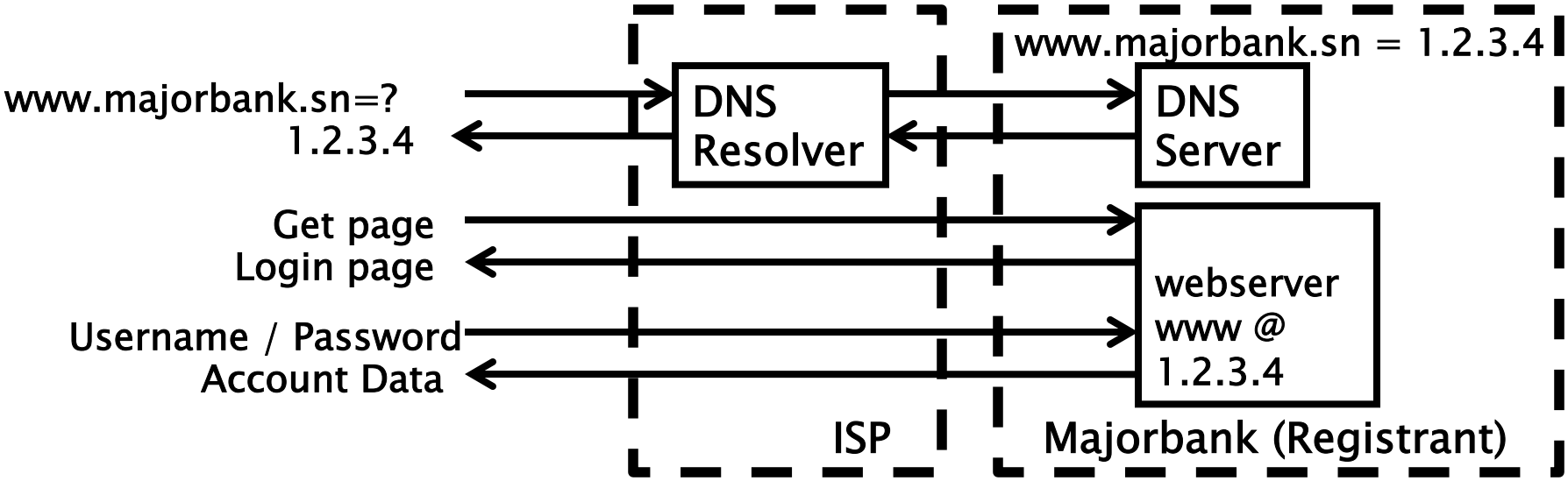
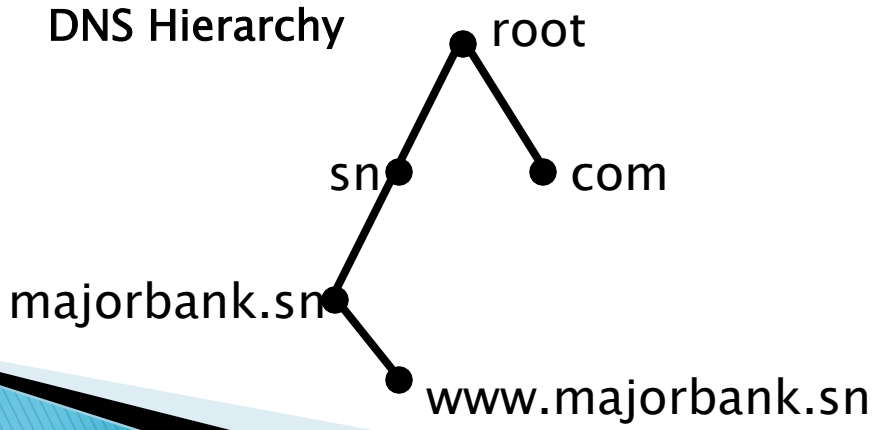
Introduction à DNSSEC

DNSSEC Roadshow,
Dakar, Senegal
20 March 2014

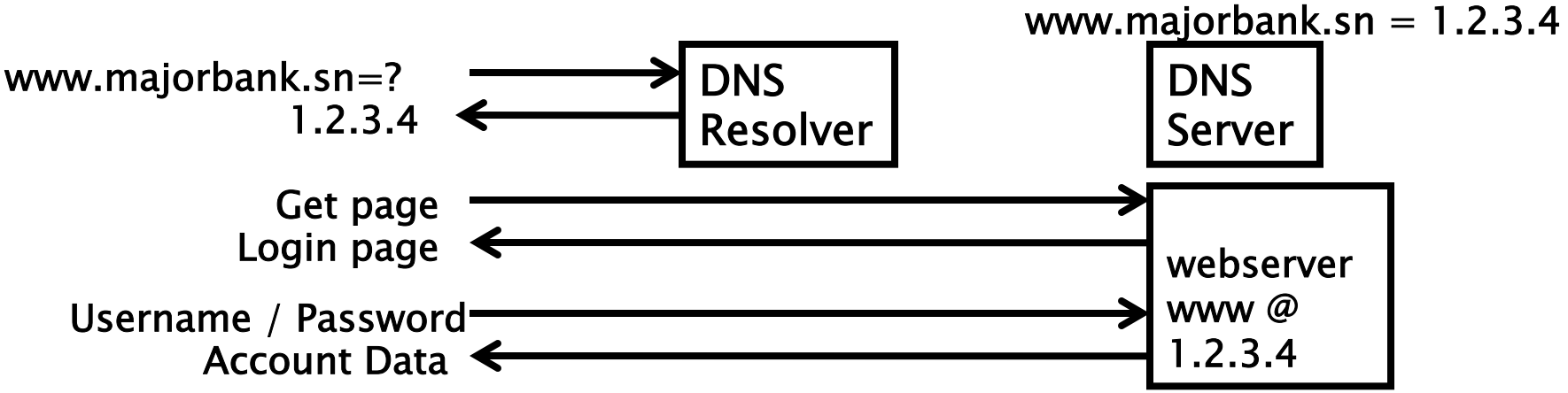
aalain@trstech.net

Annuaire téléphonique de L'Internet- Domain Name System (DNS)

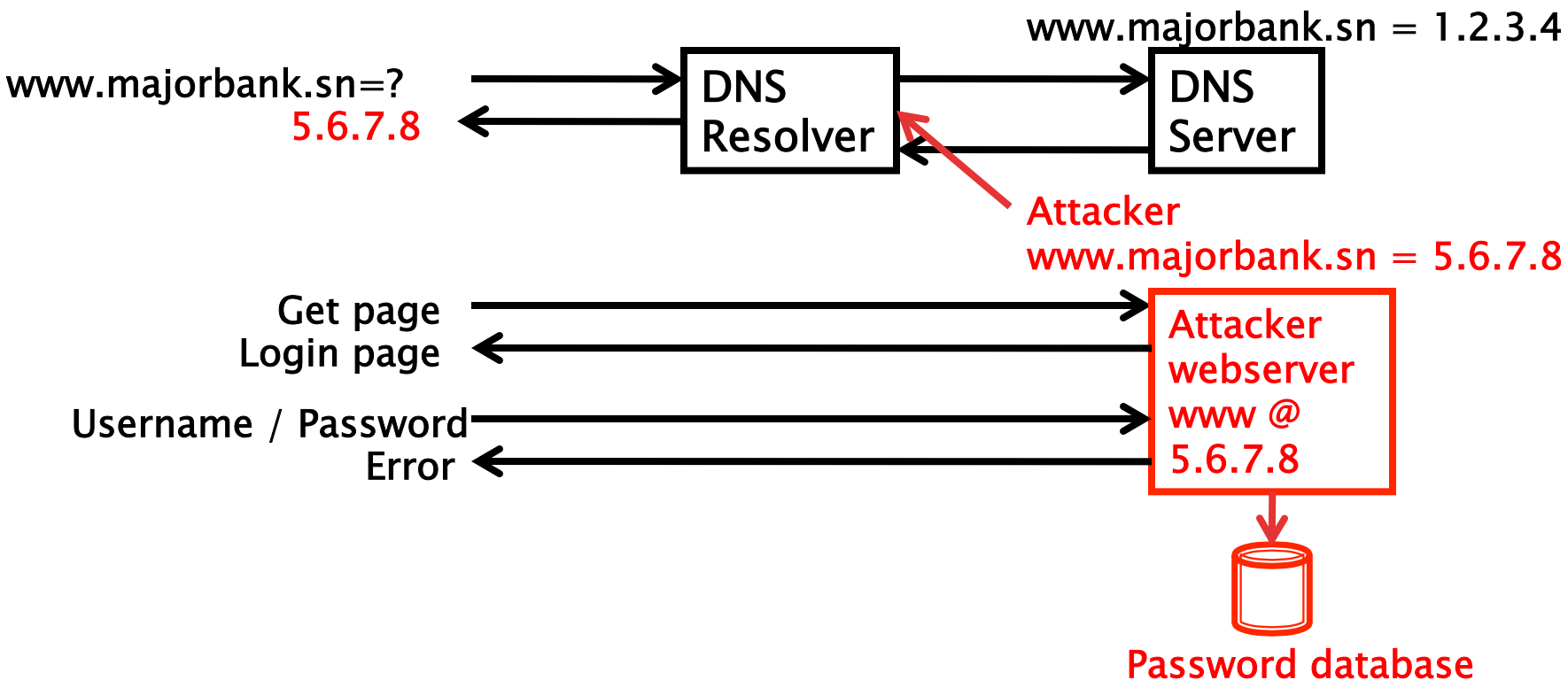




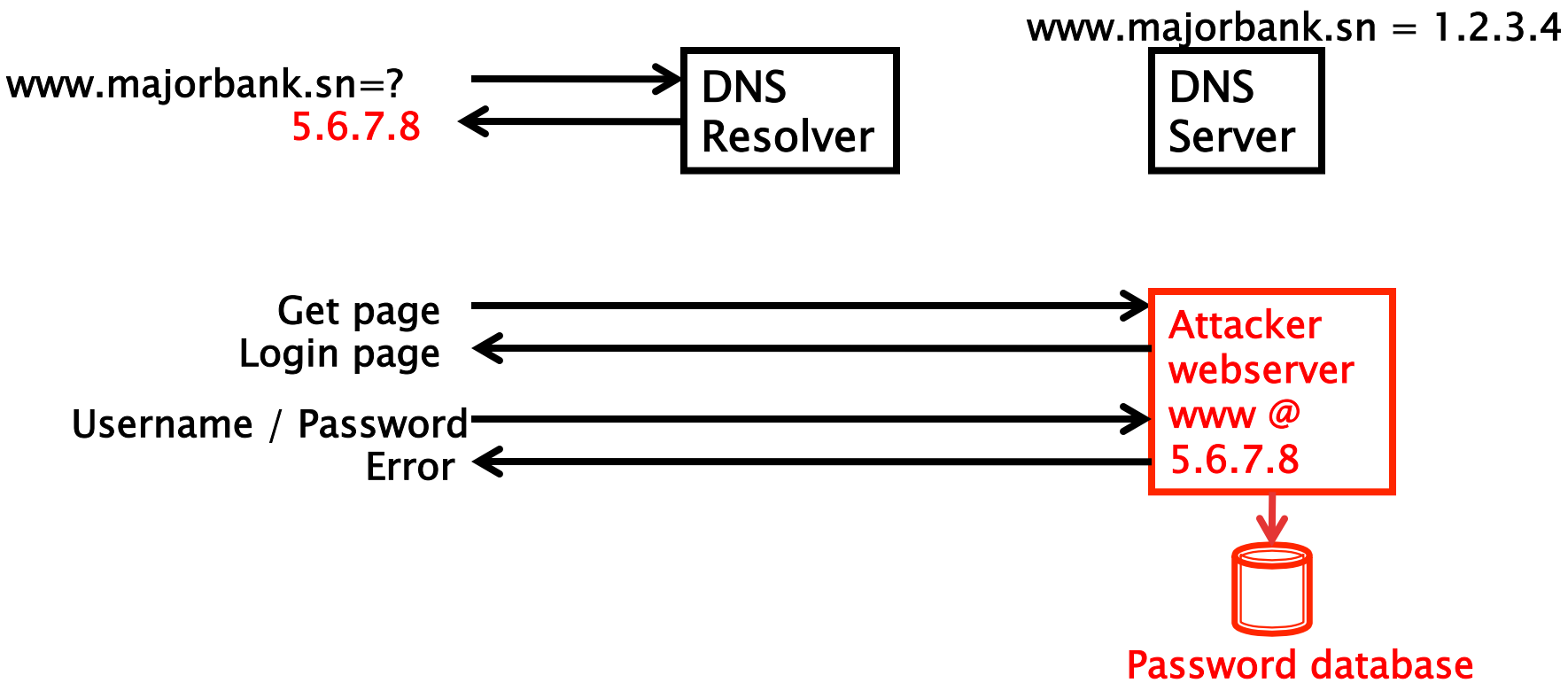
Réponses dans le cache pour efficacité



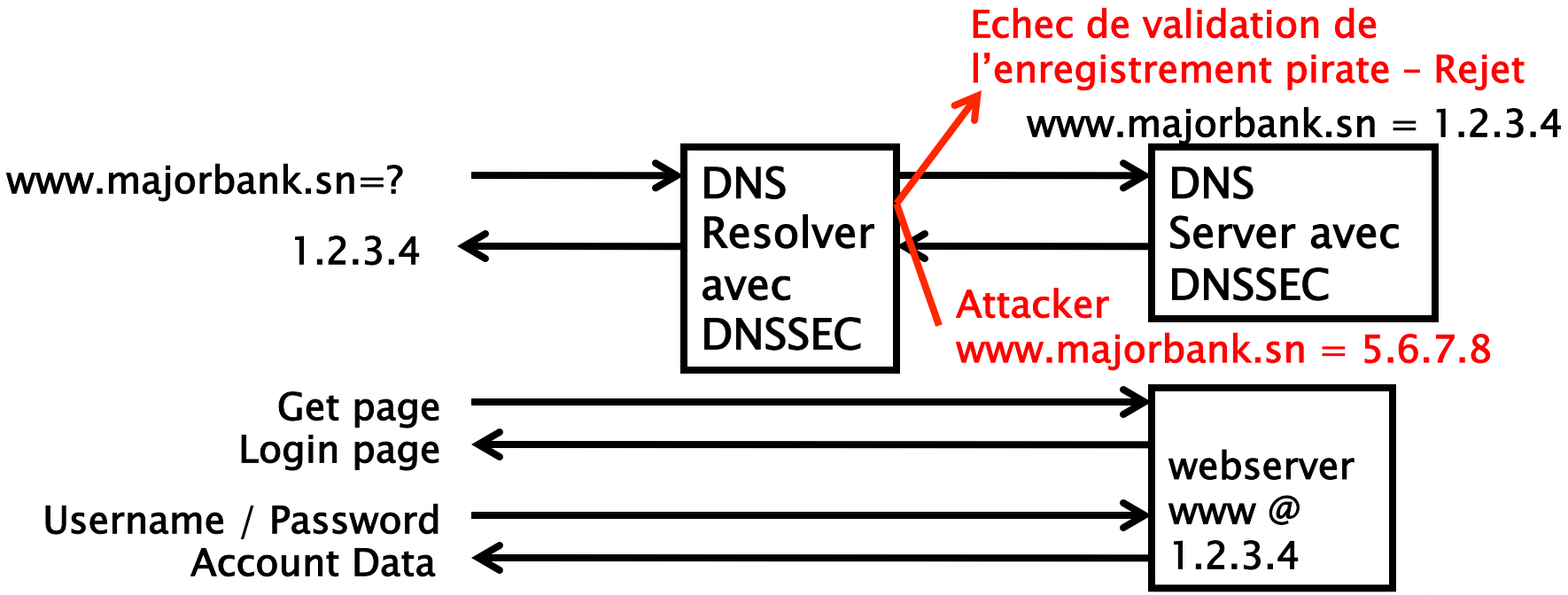
Le Problème:
Attaque d'empoisonnement du cache



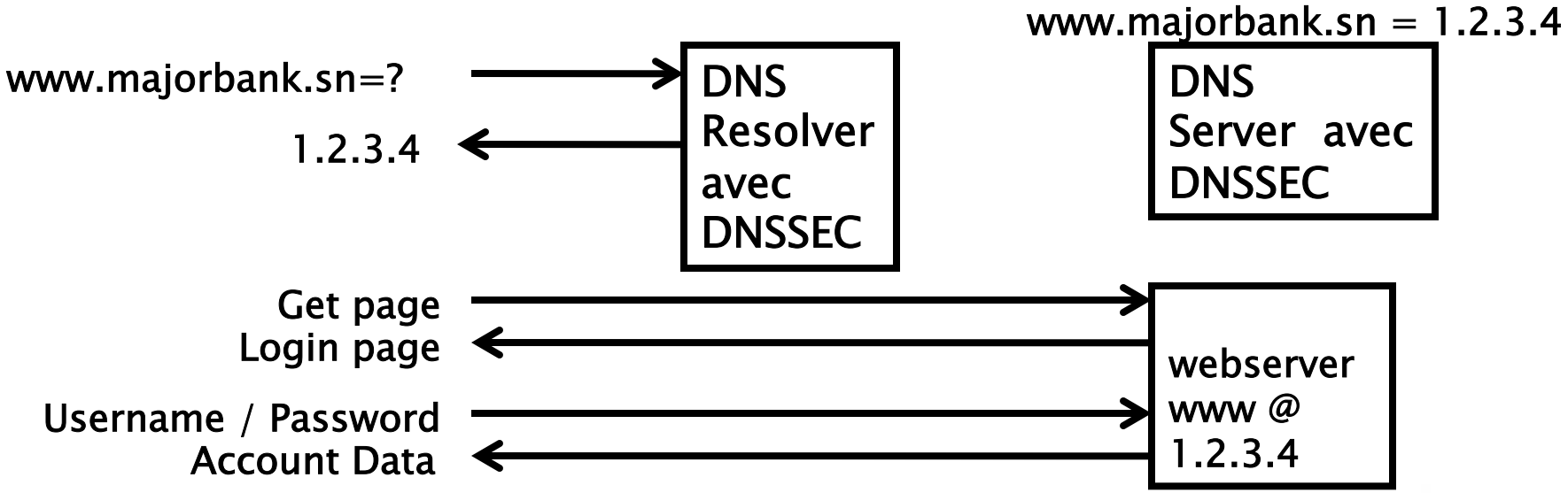
Aieeeee! Maintenant tous les utilisateurs sont renvoyés vers le pirate



Sécurisation de l'annuaire- DNS Security Extensions (DNSSEC)



Seules les réponses validées vont dans le cache

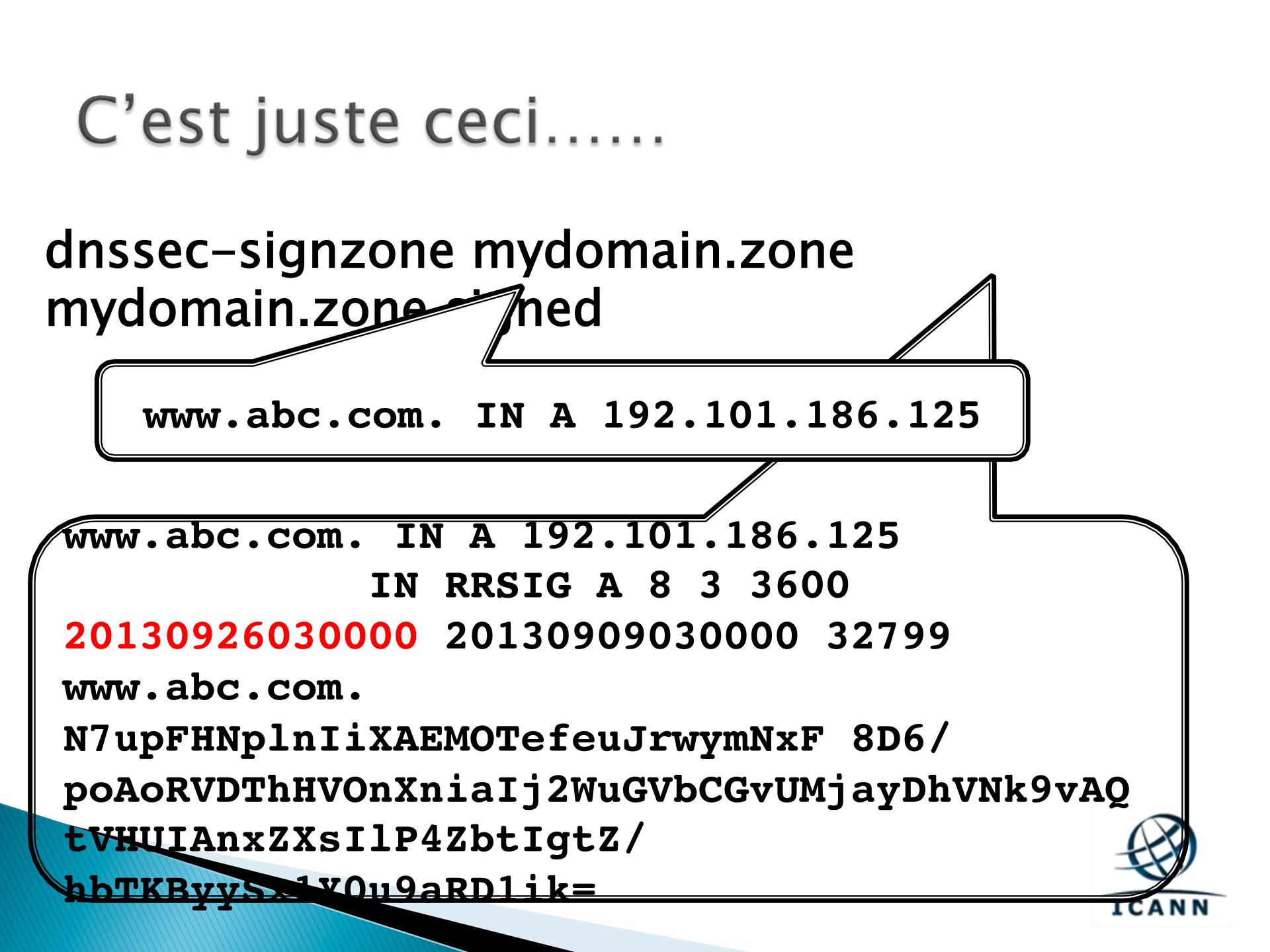


C’est juste ceci……

dnssec-signzone mydomain.zone
mydomain.zone.signed

```
www.abc.com. IN A 192.101.186.125
```

```
www.abc.com. IN A 192.101.186.125
             IN RRSIG A 8 3 3600
20130926030000 20130909030000 32799
www.abc.com.
N7upFHNplnIiXAEMOTefeuJrwymNxF 8D6/
poAoRVDThHVOnXniaIj2WuGVbCGvUMjayDhVNk9vAQ
tVHUIAnxZXsIlP4ZbtIgtZ/
hbTKByySx1Y0u9aRD1ik=
```



Un peu d'histoire

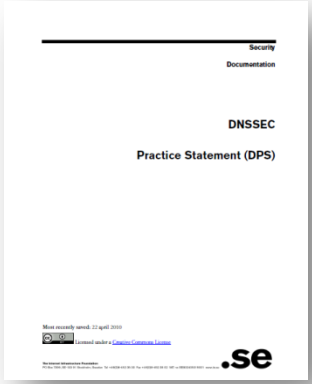
- DNS: 1983.
- Vulnérabilités decouvertes:1995
- 15+ d'années de travail à l'IETF
- 2007, certains ccTLDs ont déployé DNSSEC.
- La communauté a pressé ICANN de déployer DNSSEC à la racine
- 08/2008 Dan Kaminsky révèle des raccourcis aux vulnérabilités DNS
- La racine a été signée en juin 2010 avec une participation directe de la communauté
- Nov 2011: DNSChanger/Ghost Click: 4M de PCs dans 100 pays ont souffert de redirection. Attaque d'empoisonnement de cache d'un ISP au Brésil
- Le reconnaissance de ce ICP a provoqué le développement de solutions de sécurité innovantes au delà du DNS.

Rôles et responsabilités des acteurs: Registry, Registrars, Registrants

- Le «registrant» est responsable de la signature de sa zone et publication des clés
- Le «registrar» gère le DS (dérivé de la clé du registrant) au niveau du registre au nom du registrant
- Le «registry» génère, signe les DS des registrants et publie ses propres clés
- La racine génère, signe les DS du «registry» et publie ses propres clés.
- ISP/utilisateurs finaux utilisent copie de la clé publique de la racine pour valider de façon récursive les réponses DNS

Registrant→Registrar→Registry→Root→ISP→utilisateurs

Problèmes communs (Mais de mieux en mieux)



- Expiration des signatures: monitoring, automatisation
- Complexité: expérience, automatisation, formation
- Coût élevé des équipements: $20K→$5
- Sécurité et confiance: Accès multi-personnes transparence
- Manque du support des Registrars et ISP: sensibilisation des registrants et utilisateurs finaux
- Nombres aléatoires: meilleure considération dans les standards

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

ICANN

Références

- IETF RFCs
  RFC 4033 DNS Security Introduction and Requirements
  RFC 4034 Resource Records for the DNS Security Extensions
  RFC 4035 Protocol Modifications for the DNS Security Extensions
- ISOC Deploy360 Program

http://www.internetsociety.org/deploy360/dnssec/

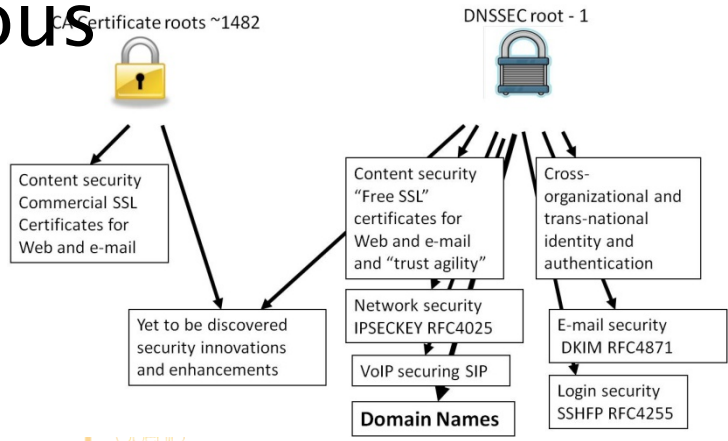
- DNSSEC Deployment Initiative

http://dnssec-deployment.org/

ICANN

Mais attendez, il y a plus…..

- DANE
  - Améliorer le TLS Web pour tous
  - Mail S/MIME pour tous
- Autres…
  - SSH, IPSEC, VoIP
  - Identité digitale
  - Autres contenus(i.e. configurations)
  - ICP Globale



+1-202-709-5262
VoIP

US-NSTIC

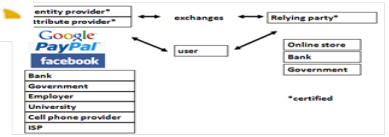
DNS is a part of all ecosystems

Google
OpenID

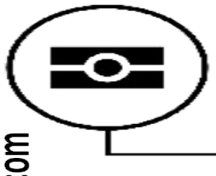
facebook

PayPal

AADHAAR



e-Passport symbol

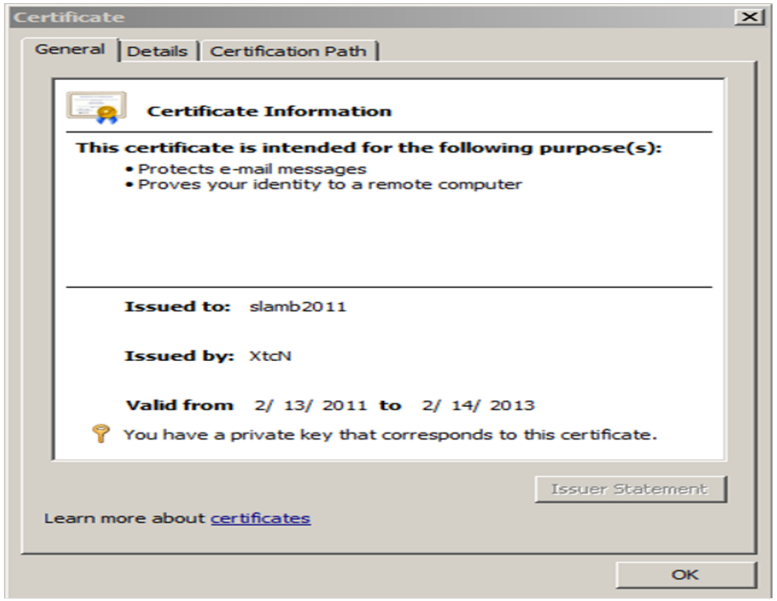


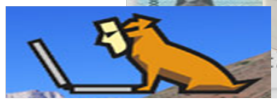
ICP Brasil
O Brasil na era da certificação digital

DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

Smart Electrical Grid





lamb@xtcn.com

En Résumé

- DNSSEC est la plus importante amélioration a l'infrastructure du coeur de l'Internet de ces 20 dernières années
- Déployer DNSSEC n'a pas besoin d'être compliqué et coûteux.
- DNSSEC ne règle pas tous les problèmes de l'Internet, mais peut constituer un important outil pour améliorer la sécurité.
- DNSSEC est une plateforme inter-organisation et transnationale pour l'innovation dans la cyber sécurité et la collaboration internationale.
- Pour bien bénéficier du DNSSEC, une plus grande campagne des registrants et utilisateurs finaux est nécessaire

Merci