Complémentarité de DNSsec et d'IPsec

Gilles GUETTE - IRISA/INRIA-Rennes

Olivier Courtay - ENST-Bretagne

Bernard COUSIN - IRISA/Univ-Rennes 1

Plan

- DNSsec
  - Rappels
  - Les bits AD et CD
- IPsec
  - Fonctionnement
- Complémentarité des deux protocoles
  - IPsec pour DNSsec
  - *Opportunistic Encryption*
  - DNSsec pour IPsec

DNSsec (1/2)

- But
  - Sécuriser le DNS
- Services de sécurité fournis par DNSsec
  - Authentification des messages DNS
  - Intégrité des enregistrements DNS
  - Intégrité des messages DNS (TSIG, SIG(0))

DNSsec (2/2)

- Serveur de noms
- Résolveur
  - DNS : il ne connaît rien de DNSsec
  - DNSsec *light* : il comprend le bit AD mais ne sait pas vérifier (cryptographiquement) un enregistrement DNSsec
  - DNSsec *full* : il comprend et sait vérifier (cryptographiquement) les enregistrements DNSsec

Les bits AD et CD

- AD : *Authenticated Data*
  - Tous les enregistrements de la réponse ont été vérifiés par le serveur de noms.
  - Croire le bit AD nécessite un canal sécurisé entre le serveur de noms et le résolveur

- CD : *Checking Disabled*
  - Des enregistrements non vérifiés sont contenus dans le message DNS

Utilisation des bits AD et CD

- Le bit AD permet d'avoir des résolveurs plus léger (au sens cryptographique)

- Le bit CD positionné dans une requête indique que des enregistrements non vérifiés sont acceptés

IPsec (1/3)

- Mécanismes IPsec
  - *Authentication Header* (AH)
  - *Encapsulation Security Payload* (ESP)
  - IP *compression* (IPcomp)
- Services de sécurité rendu
  - Authentification (AH, ESP)
  - Intégrité (AH, ESP)
  - Confidentialité (ESP)

IPsec (2/3)

- Fonctionnement :
  - *Security Policy Database* : stocke les politiques vis à vis des communications (ensemble des paramètres possibles d'une connexion)
  - *Security Association* : un contexte (ex : avec @IP chiffrement 3DES authentification MD5)
  - *Security Association Database* : conserve les contextes des communications

IPsec (3/3)

- Une application initie une communication
- Les systèmes/noyaux négocient les attributs
  - Paramètres cryptographiques (3DES, ...)
  - Échange des identités (X.509)
- Les applications peuvent communiquer

Remarques sur IPsec

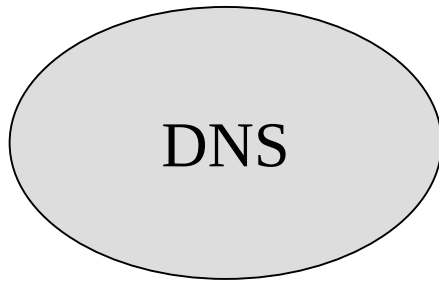
- On peut utiliser :
  - Un secret partagé
  - Des certificats X.509
    - Utilisation d'une PKI
    - Gestion de CRL

Complémentarité

- IPsec pour DNSsec
  - Sécurisation des communications entre un résolveur *light* et un serveur de noms

- DNSsec pour IPsec
  - Utilisation de la chaîne de confiance DNSsec pour récupérer et vérifier les clés nécessaires à IPsec

IPsec pour DNSsec (1/2)



Application

Requête/réponse DNS

Résolveur

Serveur DNSsec

User space

Kernel space

IPsec

IPsec

IPsec pour DNSsec (2/2)

- Avantages :
  - Avoir des résolveurs plus légers
  - Utiliser le bit AD
  - Les communications entre les résolveurs *light* et les serveurs de noms sont sécurisées
  - Réponse plus rapide du résolveur (pas de traitement cryptographique)
  - Indépendance des résolveurs par rapport aux algorithmes cryptographiques utilisés

Remarques

- IPsec récupère les clés publiques *via* des certificats (X.509)

- Il existe un autre moyen
  - Récupérer les clés *via* DNS(sec)
  - L'*opportunistic encryption*

Opportunistic Encryption (1/2)

- Faire de l'IPsec «automatique»
- Établir une connexion sécurisée entre 2 machines qui ne se connaissent pas
- 1 seule implémentation : FreeSwan 2.0X
- 2 modes de fonctionnements :
  - *Host-to-Host*
  - *Security Gateway*

Opportunistic Encryption (2/2)

- Toutes les informations nécessaires sont stockées dans le DNS (TXT RR)

Forward DNS record

```
; RSA 2192 bits   xy.example.com   Thu Jan  2 12:41:44 2003
IN     TXT     "X-IPsec-Server(10)=@xy.example.com" "AQOF8tZ2... ...+buFuFn/"
```

Reverse DNS TXT record

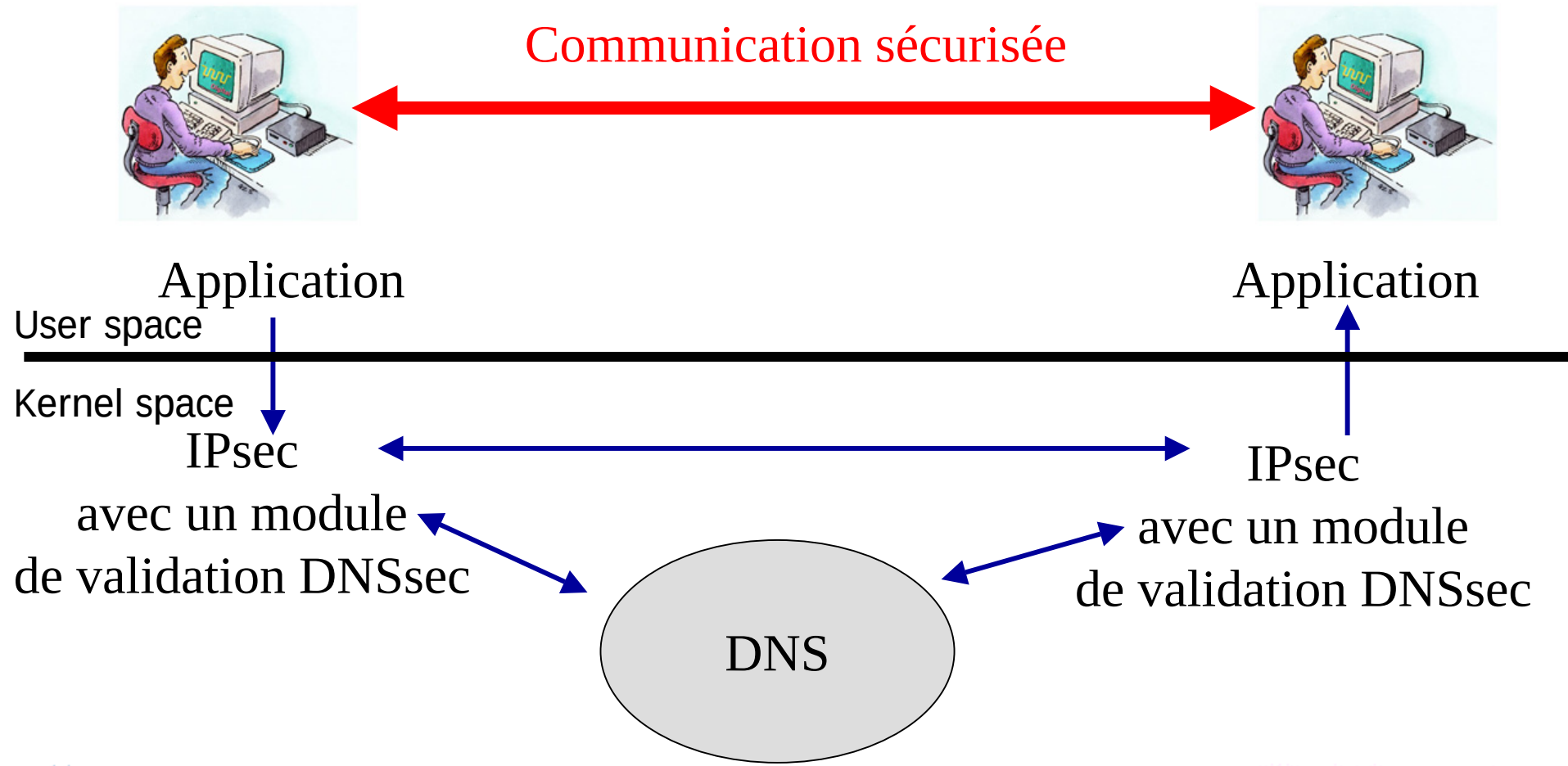
```
; RSA 2048 bits  xy.example.com   Sat Apr 15 13:53:22 2000
IN TXT  "X-IPsec-Server(10)=192.0.2.11" " AQOF8tZ2...+buFuFn/"
```

Problème de démarrage

- Le bit AD nécessite de l'IPsec
- IPsec nécessite DNSsec

- Installer un module DNSsec full dans le module IPsec

DNSsec pour IPsec (1/2)



DNSsec pour IPsec (2/2)

- Avantages :
  - Pas besoin de connaître la machine *a priori*
  - Disponibilité des clés
  - Clés vérifiables par la chaîne de confiance DNSsec (grâce aux signatures des RR)
  - Pas de CRL à gérer ou à consulter
  - Procédé transparent pour l'utilisateur
  - Déploiement simplifié pour l'administrateur

Configuration nécessaire

- Placer les clés publiques IPsec dans le fichier de zone
- Placer les clés publiques/privées sur la machine
  - Indispensable pour utiliser la cryptographie à clés publiques
  - Configuration minimale

Conclusion

- Résolveur plus léger
- Communications sécurisées avec des résolveurs *light*
- Disponibilité des clés pour IPsec
- Bonne complémentarité des deux protocoles
- Peu de configuration
- Transparent pour l'utilisateur

Perspectives

- Étendre le fonctionnement au mode passerelle de sécurité
- Intégration dans FreeSwan (notre patch est actuellement en test chez FreeSwan)

Questions