NETASQ
secure internet connectivity

Faiblesses d'IPSec en déploiements réels

(Bypassing IPSec gates for dummies with scapy for fun and profit)

VANHULLEBUS Yvan
vanhu@netasq.com

SSTIC 06

Au programme...

- vanhu@darkstar ~$ finger vanhu
- Présentation (très) rapide d'IPSec
- Classification des faiblesses
- Faiblesses des protocoles
- Problèmes d'implémentations
- Problèmes de déploiements
- Conclusion

Pas de panique !

- Explications détaillées d'IPSec dans les actes
  - Explications rapides dans les slides
- Pas de “zero day”, pas de shellcode
- Pas de démo “murphy”
  - Aucun paquet maltraité pendant cette présentation !
- Pas de logo “Rstack”…
- Le gentil gagne à la fin……
  - Mais devra surement modifier sa configuration !!!
- Rennes – Paris a 18h…..

vanhu@darkstar ~$ finger vanhu

- NETASQ (~~Firewalls~~ ~~IPS~~ UTMs Appliances)
  - Chef de projet IPSec
- Développeur ipsec-tools (http://ipsec-tools.sf.net)
- Développements sur la pile IPSec KAME (FreeBSD)
- Google: vanhu + CV + feeling lucky

IPSec pour les nuls (en 5 minutes)

Objectifs d'IPSec

- Prévu pour relier des réseaux distincts
  - “table de routage” supplémentaire: SPD
  - Plusieurs extrémités de traffic possibles vers une extrémité de tunnel
- Protection du traffic IP: ESP / AH
- Negociation dynamique de clés
  - Clés statiques possibles (obsolète / “debug”)
- Algorithmes et protocoles “standards”

Fonctions fournies

- Confidentialité des données
  - Chiffrement
- Intégrité des données
  - Hashs
- Authentification
  - Identification fiable et mutuelle des correspondants

Utilisations d'IPSec

- Relier des réseaux
  - Agences via xDSL
- Postes nomades
- Sécurisation de flux non surs (NFS, etc...)
- VoIP, etc...
- Obligatoire dans IPv6
  - “End to End”

Avantages d'IPSec

- Identification forte des correspondants
- Encapsulation au niveau IP
- Protocoles normalisés par l'IETF
  - Protocoles publics et audités
  - Interopérabilité
- Tunnels “sur le chemin”
- Possibilités de topologies complexes

Inconvénients d'IPSec

- Complexe à mettre en oeuvre
  - Déploiements nécessitent des connaissances en IPSec
  - Problèmes d'implémentations
    - Bugs....
    - Problèmes d'interopérabilité....
- Couts des logiciels ?
- Problèmes de routage d'ESP et AH
  - difficilement compatibles avec le NAT
  - Parfois bloqués par des routeurs

Encapsulation des données

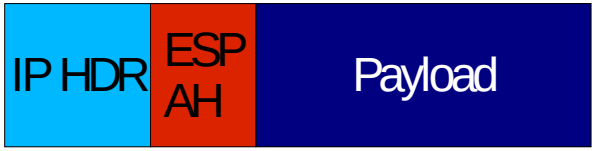
- Mode Tunnel
  - Relier des Réseaux RFC1918 (non routables) au travers d'un réseau routable
  - “Host to Net”, “Net to Net”
  - Overhead plus important (1 header IP)
- Mode Transport
  - “Host to Host” uniquement
  - Extrémités doivent pouvoir se contacter (routage)

Encapsulation des données (suite)

Paquet d'origine

Mode Tunnel

Mode Transport



Encapsulation des données (fin)

- ESP
  - Chiffrement des données
  - Hash optionnel des données
- AH
  - Hash uniquement
  - Couvre aussi l'en-tête IP et l'entete AH

Négociation dynamique: IKE

- RFCs 2407, 2408 et 2409
- Phase 1 (Main mode / Aggressive mode)
  - Authentification mutuelle des correspondants
  - Mise en place d'une “Isakmp SA”
  - Echange de clés par Diffie-Hellman
- Phase 2 (quick mode)
  - Négociation de “IPSec Sas”, qui protègeront le traffic IP
  - Protégée par la Isakmp SA
  - Plusieurs phases 2 possibles pour un correspondant

Extensions IKE

- Xauth
- Mode Config
- Dead peer detection
- NAT-Traversal
- etc...

IKEv2

- Simplifications des protocoles
  - Plus de DOIs
  - 1 seul mode de phase1
  - Opérations cryptographiques faites par l'initiateur en premier
- Pas d'implémentation “opérationelle”
  - Probablement des erreurs de programmation similaires
- Probablement autant d'erreurs de configuration

Différents types de faiblesses

Catégories de menaces

- Déni de service
  - Bloquer les négociations ultérieures
  - Bloquer immédiatement le traffic
- Corruption de données
  - Modifications aléatoires
  - Modifications controllées
- Interception de données
- Accès non autorisés

Autres critères de classification

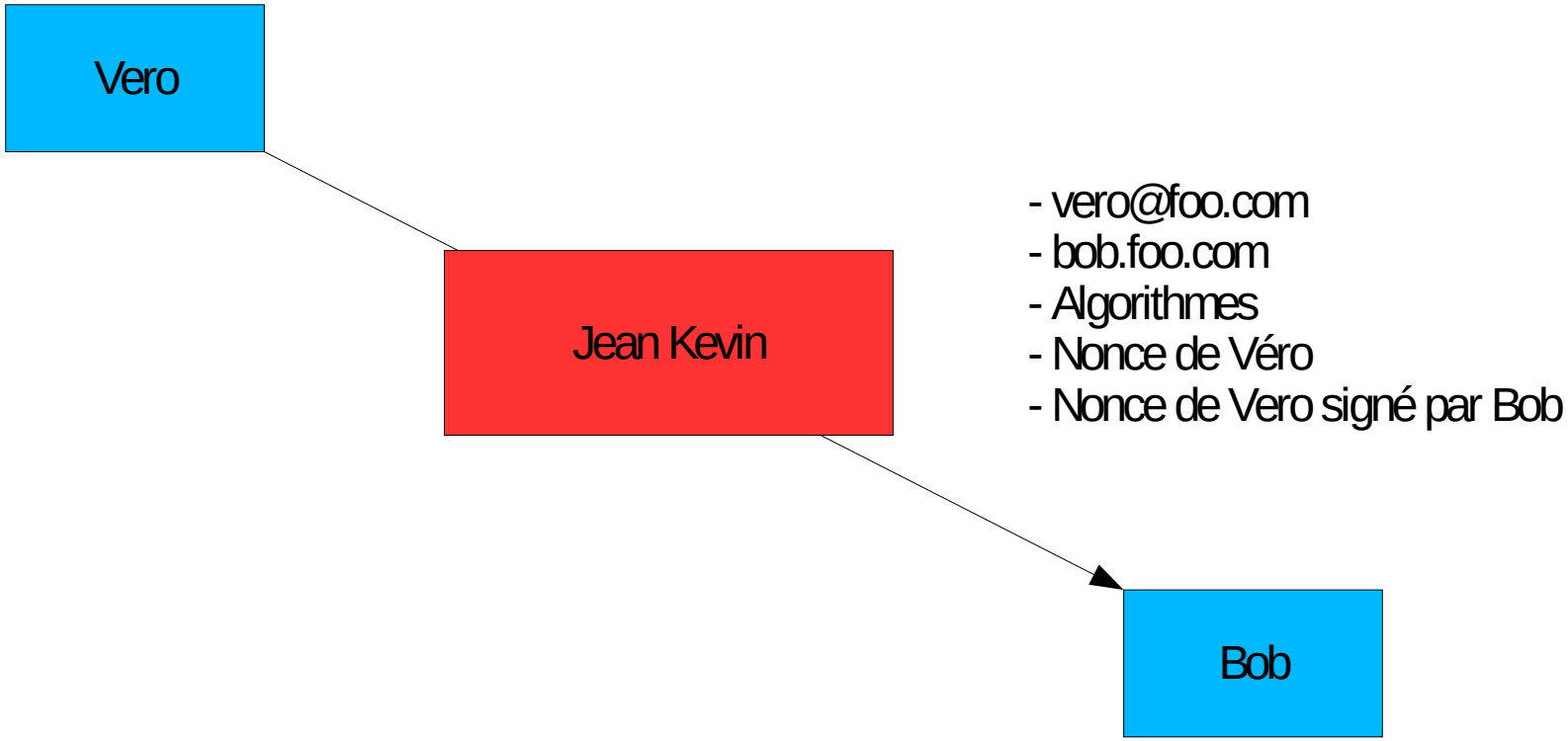
- Temps requis pour l'attaque
  - A comparer avec la durée de vie des données
- Accès prérequis
  - Correspondant IPSec légitime
  - Correspondant révoqué
  - Aucun prérequis
- Ressources nécessaires à l'attaquant

Faiblesses des protocoles

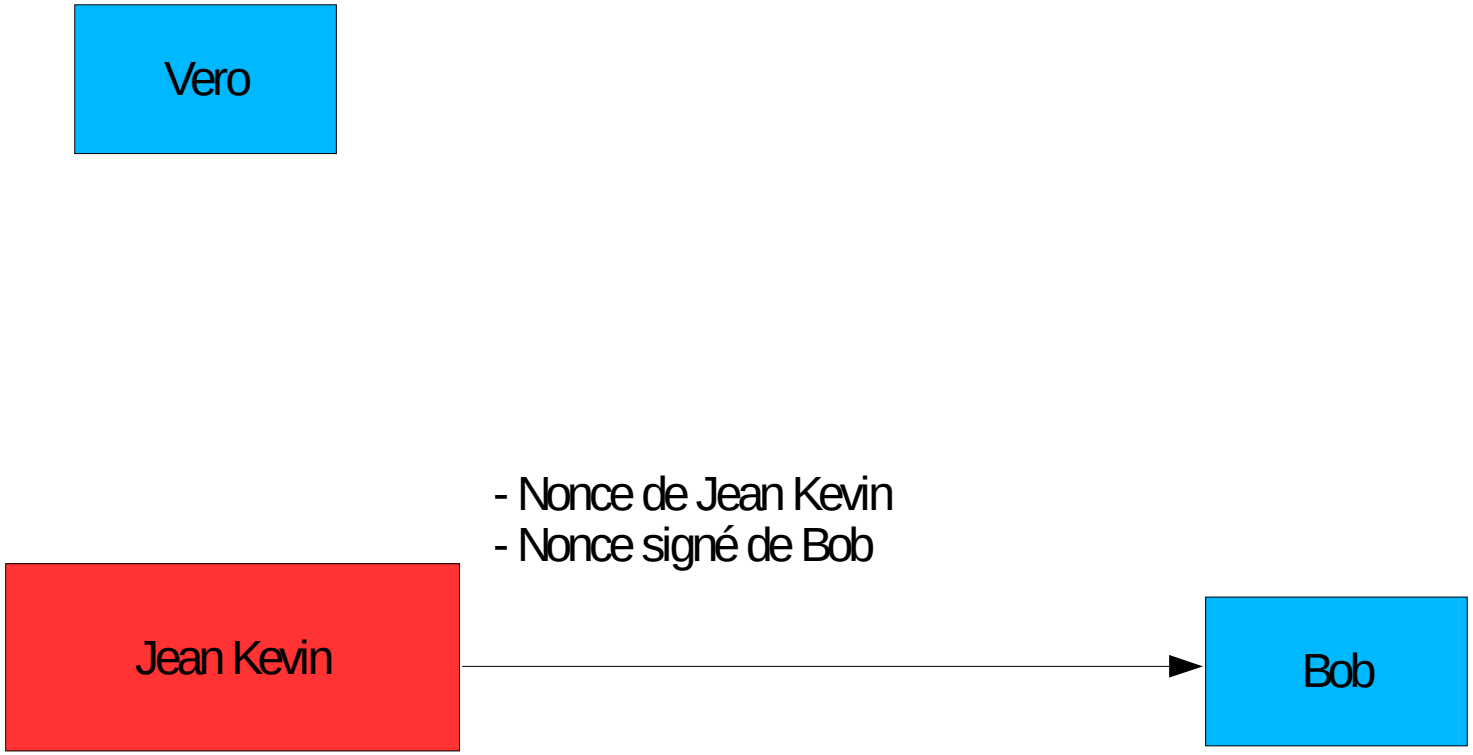
Mode Aggressif et secret prépartagé

- Mode aggressif
  - le répondeur est le premier à utiliser des secrets
  - Les signatures d'aléas ne sont pas chiffrées
  - Possibilité de commencer une négociation pour obtenir une signature par le répondeur
- Avec un secet prépartagé: attaque par force brute possible sur la signature récupérée

Mode Aggressif et secret prépartagé (2)



Mode Aggressif et secret prépartagé (3)



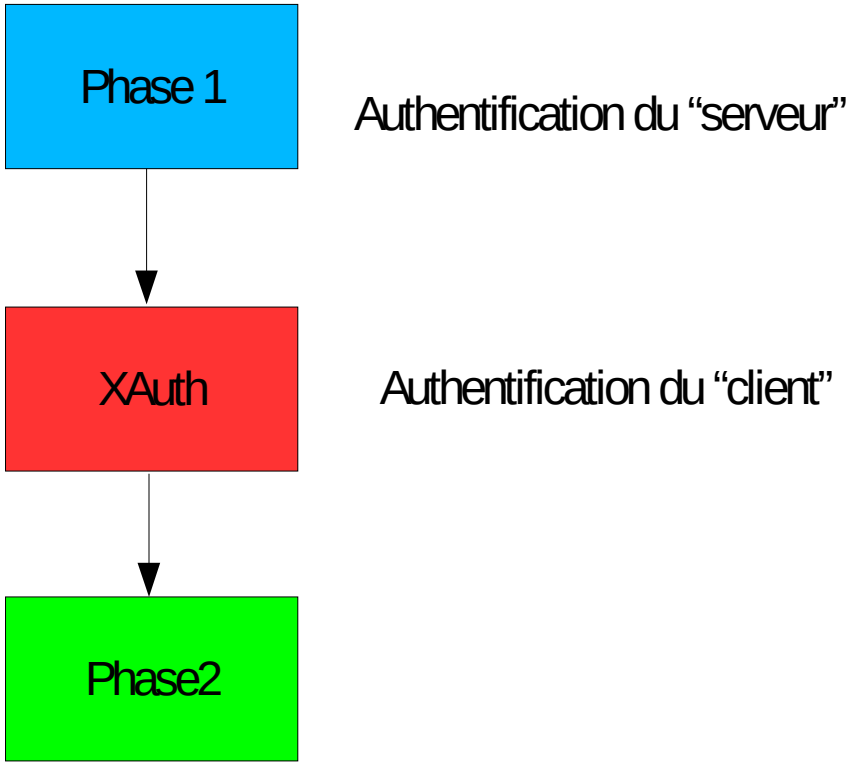
Mode Aggressif et secret prépartagé (4)

- Proposition valide
  - Transform1: DES / MD5
  - TransformX: .....
- Durée de vie valide
  - Durée de vie très courte
- Identifiant valide
  - vero@foo.com
  - vero.w@foo.com
  - pub@ed-diamond.com
  - .....

Liens entre les clés de sessions

- Par défaut, les clés de sessions des IPSec SAs sont dérivées les unes des autres
  - Casser une clé permet de facilement calculer les suivantes
- Solution: utilisation du “PFS”
  - Regénération de clés indépendantes par Diffie-Hellman

Authentification faible: Xauth (1)



Authentification faible: Xauth (2)

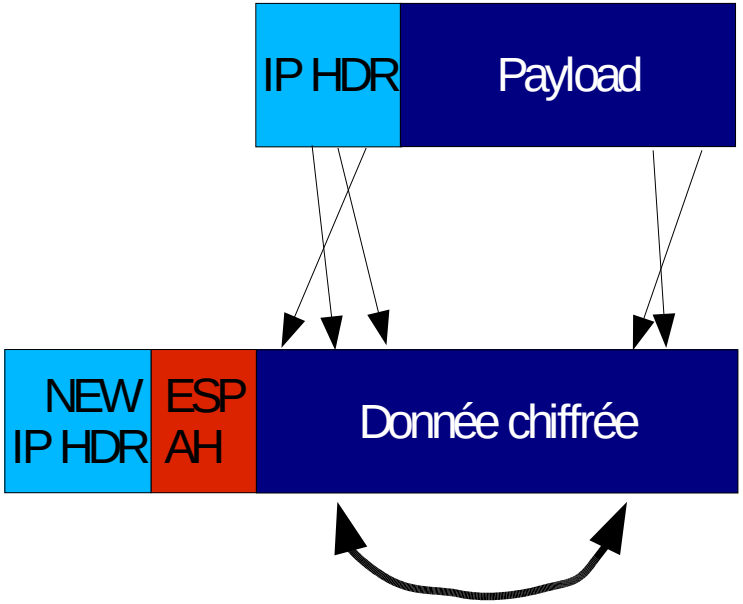
- En théorie: Xauth protégé par la phase 1
- En pratique: phase 1 affaiblie
  - algorithmes faibles
  - clé “de groupe”
  - clé simpliste
- Reste fiable avec authentification du “serveur” par certificat en phase 1

ESP et permutation de bits

- En CBC, possibilités de permutation de certains bits
  - La donnée reste déchiffrable
  - On peut calculer quels bits sont permutés dans la donnée en clair

ESP et permutation de bits (2)

- Localisation des bits “intéressants”
  - En-tete IP encapsulée
  - Position dans le paquet déchiffré prévisible



ESP et permutation de bits (3)

- “Facile” de changer des données en aveugle
- Difficile à exploiter en pratique
  - Changer l'IP pour une adresse maitrisée
    - Nécessite de connaitre l'IP à modifier
  - Etre juste en sortie de réseau
    - Le paquet doit de toutes facons etre bloqué par la pile IPSec
- Solution simple: utilisation d'un algorithme de hash (MD5, SHA1)

Solutions ?

- Connaitre ces faiblesses !
- Interdire leur utilisation par défaut ?
  - ipsec-tools: ./configure --enable-unsafe ?
  - Avertissements dans les interfaces ?
  - Alarmes sur les I(D|P)S ?

Faiblesses d'implémentations

IPSec statique

- Clé unique non renouvelée
  - Difficultés de maintenance
  - Difficultés de répudiation
  - Attaques statistiques deviennent très plausibles
- Seul mode supporté par certains routeurs
- Seul mode que certains administrateurs savent configurer.....

Analyse IKE

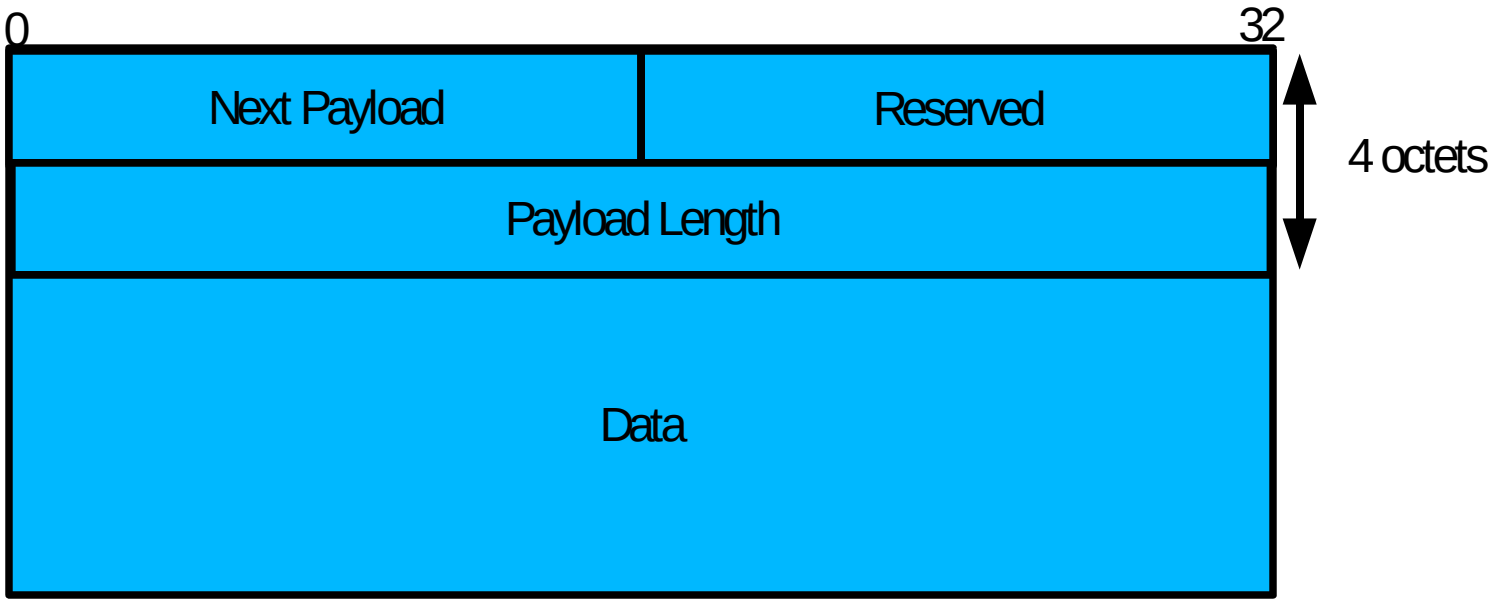
- IKE complexe à traiter
  - Données binaires
  - Données de tailles variables
  - Nombreux types de données
  - Données obligatoires ou optionnelles selon les cas

Faiblesses de l'analyse IKE

- Test “Protos”
  - Denis de services souvent simples à exploiter
  - A peu près toutes les implémentations touchées
    - Pas toujours directement exploitable avec les configurations par défaut
- Accès non autorisés
  - CISCO 64424
- Execution arbitraire de code
  - Checkpoint CVE-2004-0469

Exemple: Gestion des payloads Isakmp

Structure d'un payload Isakmp:



Exemple: Gestion des payloads Isakmp (2)

```
/* Dans le code: */

        if(isakmp->tlen <= 0)
                return;

        p=malloc(isakmp->tlen-4);
        memcpy(p, isakmp->data+4, tlen - 4);
```

Exemple: tailles des données (ASM)

```
; test...
: ....
movl   -4(%ebp), %eax
subl   $4, %eax
movl   %eax, (%esp)
call   malloc
movl   %eax, -8(%ebp)
; memcpy...
```

Exemple: Gestion des payloads Isakmp (3)

- tlen < 0: testé
- tlen > sizeof(UDP): testé
- tlen > 0 && tlen <=4 ??
- malloc(-1) / malloc(-4)

Configurations par défaut

- Durées de vies trop élevées
  - Parfois 1 semaine pour une phase1
- Algorithmes “faibles”
  - DES, pour compatibilité
- ESP sans algorithme de hash
  - Bit flipping

Validations faibles

- racoon: mode de vérification “obey”
  - Accepte toute proposition du correspondant
- Utilisé dans tous les exemples il y a encore peu
- En pratique:
  - “I just set up my configuration in obey mode, and now it works. thanks guys” ((C) Anonymous / Ipsec-tools ML)

Validations incomplètes des paquets

- Mauvaise validation du Hash ?
- Séquence d'anti rejeu mal gérée ?
- Confrontation du paquet décapsulé par rapport à la police de sécurité
  - Source
  - Destination
  - Passerelle correspondante
  - Linux / AH / Transport: pas de test (vu au SSTIC 05 :-)

Failles dans le traitement des paquets

- Déni de service
  - KAME: test inversé
  - Un paquet AH malformé génère un appel a panic()
- Exécution de code
  - OpenBSD: CVE-2001-0284
  - Paquet AH malformé

Configurations complexes

- Eléments implicites
  - Extrémités de traffic calculées (Checkpoint)
  - Choix des certificats obscur (Checkpoint)
- Configurations trop lourdes
  - Isakmpd
    - 10 sections de configuration pour 1 tunnel !
    - un Isakmpd.policy incompréhensible
  - KAME / Linux 2.6 + racoon
    - Liens peu évidents entre les différents éléments de configuration

Problèmes cryptographiques

- Sécurité d'IPSec basée sur la cryptographie
- La qualité de la couches cryptographique est importante !
- Ex: Cisco CVE-2002-1105
  - Génération d'aléa faible
  - Attaques par usurpation d'identité

Problèmes annexes

- Passerelles IPSec souvent intégrées
  - Appliances
  - Linux / BSD box “à tout faire”
  - Postes clients
- Faiblesses avant et après IPSec
  - Récupération de configuration
  - Interactions du démon (LDAP, fichiers, NFS, etc...)
  - Détournement d'autres outils
  - Etc...

Fuites d'informations

- VendorID: signature “évidente”
- Scapy: ikescan(“192.168.0.0/16”)
- Ikescan
  - Analyse du VID

Solutions ?

- Développeurs
  - Programmer mieux ?
  - Tests fonctionnels (PROTOS, Scapy, etc...)
  - Audits de code (Coverity, etc...)
  - ./configure --enable-nobugs ?
- Utilisateurs
  - Surveiller les listes, annonces, nouvelles versions
  - Sécurité au quotidien

Problèmes d'interface “chaise/clavier”

Tunnels sans filtrage

- Un tunnel IPSec garantit que le trafic qui part arrive “bien”
- Aucune garantie sur le trafic en question
- Un poste mobile peu sur peut compromettre tout le réseau

Mauvaise compréhension des configurations

- “Require” KAME
  - Utilisé dans tous les tutoriels
  - Ne garantit pas une correspondance forte entre configuration et police de sécurité
  - En pratique, flux “mal” protégés possibles
- Solution: “Unique”
  - Lie la SA négociée avec la SPD qui l'a demandée

Secrets mal protégés

- Configurations accessibles
  - Fichiers rw-rw-rw-
  - Base de registres lisible
- “Hi guys, here is my configuration, with valid IP addresses and real preshared keys in the dump, can you help me ?” ((C) Anonymous / ipsec-tools ML)

Mauvaise gestion de PKIs

- Clé privée de CA mal protégée
- Certificats non révoqués
- CRLs non générées
- CRLs valables 10 ans

Solutions ???

- Communiquer sur ces problèmes
- Documentation
- Communiquer sur ces problèmes !
- ./configure --disable-boulet ?
- Communiquer sur ces problèmes ?

Questions ?

(pas trop fort, merci)