Chapitre 5 : Sécurité de la c
réseau

(sécurité et parallélisme)

Plan

- Description d'IPSec
- ISAKMP
  - IKE
  - SA
  - OAKLEY
- AH et ESP
- Annexes

1. Description d'IPsec

- Objectif
- Principe
- Architecture
- Protocoles

IPSec

- IPSec = IP Security
  - initialement défini pour IPv6
  - à présent utilisé comme complément à
- Objectif
  - fournir l'autentification, l'intégrité et le ch
- Principe
  - applicable par un noeud intermédiaire
  - transparent pour les hôtes

IPSec

- Architectures (RFC 4301)
  - routeur / routeur : habituel pour un VPN
  - hôte / hôte : communication bidirectionn
  - hôte / routeur : accès à un réseau
- Protocoles d'IPSec
  - transport : AH et ESP
  - échange et gestion des clés : ISAKMP

2. ISAKMP

- ISAKMP
- IKE
- SA
- OAKLEY

ISAKMP

- ISAKMP = Internet Security Associati
  Key Management Protocol
  - RFC 2408
  - cadre générique, ne définit pas forcéme
    d'algorithme
  - autentification de l'entité distante, gestio
    paramètres de sécurité, génération des
    réduction des attaques

ISAKMP

- Utilisation d'IKE initiale
  - IKE est utilisé pour négocier les paramè
    et produire trois clés : clé d'autentificatio
    chiffrement et de production d'autres cle
- Types de clés
  - clés de sessions : durée de vie courte
  - clés de chiffrement de clés : durée de v

ISAKMP

- Propriété : perfect forward secrecy (F
  - les clés de sessions passées ne peuve
    devinées si un secret à long terme est c
- Propriété : back traffic protection
  - chaque clé générée est indépendante c

IKE

- IKE = Internet Key Exchange
  - protocole utilisé pour installer des SA
  - UDP, port 500
  - utilise OAKLEY
- Phases
  - établissement d'un canal sécurisé auten
  - établissement de SA

SA

- SA = Security Association
  - association de sécurité
  - gère les paramètres des algorithmes cryptographiques (taille des clés, algorit durée de vie des clés, etc.)
- Principe
  - SA unidirectionnelle et unique
  - une entité mobile établit une seule SA a entité fixe, valable pour plusieurs servic

SA

- Caractérisation
  - SA caractérisée par SPI (Security Paran
    + adresse destination + protocole (AH e
  - SPI transmis dans chaque paquet
  - SPD (Security Policy Database) = asso
    un paquet et des SA, agit comme un fir
  - SAD (Security Association Database) =
    données des SA

SA

- Pour chaque paquet IPSec
  - traitement par le SPD : obtention d'un o SPI
  - consultation de la SAD pour chaque SP de une ou plusieurs SA
  - traitement en fonction des SA

OAKLEY

- OAKLEY
  - échange de clés basé sur Diffie-Hellma
  - protection contre des attaques de rejeu nonce) et de déni de service (cookie : fa autentification mais stockage limité)
  - autentification contre l'homme au milieu
- Utilisation
  - avec ISAKMP
  - directement sur IP

OAKLEY

- Autentification
  - signatures (par certificats)
  - chiffrement (par PKI)
  - clés pré-partagées (manuel)
- Protocoles similaires plus anciens
  - Photuris
  - SKEME

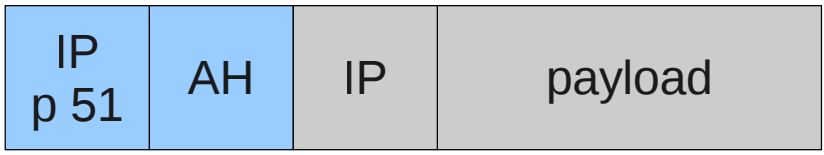
2. AH et ESP

- AH
- ESP
- modes d'IPSec
  - transport
  - tunnel

AH

- AH = Authentication Header
  - RFC 2402
  - dispose d'un entête au-dessus d'IP
- Fournit l'autentification, l'intégrité du p
  complet et l'anti-rejeu
- Utilisation
  - mode transport :

  - mode tunnel :



AH

- Mécanisme
  - numéro de séquence
  - champ d'autentification (hachage signé)
  - assure l'intégrité de l'ensemble du paqu
    les champs modifiables)

ESP

- ESP = Encapsulating Security Payloa
  - RFC 2406
- Fournit la confidentialité, l'autentificat l'intégrité et l'anti rejeu
- Utilisation
  - similaire à AH

ESP

- Mécanisme
  - numéro de séquence
  - champ d'autentification (hachage signé)
  - chiffrement
  - chiffrement et intégrité uniquement sur

IPSec en mode transpo

- Diagramme : hôte à hôte
- Utilisation
  - AH et/ou ESP
  - sécurisation de communications de bou (de client à client)
  - adresses sources et destinations visible réseau public
- Utile quand les réseaux internes n'on besoin d'être sécurisés
- Problème avec NAT + AH (intégrité e

IPSec en mode tunne

- Diagramme : tunnelling
- Utilisation
  - AH et/ou ESP
  - contrôle d'intégrité sur l'ensemble du pa AH)
  - données chiffrées (via ESP)

Algorithmes cryptographi

- Intégrité
  - SHA1
- Autentification
  - HMAC
- Chiffrement
  - 3-DES
  - AES

Annexes

- Annexe 1 : sécurité logicielle

Annexe 1 : sécurité logic

- Buffer overflows
  - description (pile, empilage des paramèt variables locales)
  - shellcode (cinquantaine d'octets)
  - protections : fonctions "n", langage (Jav vérification de code, audit, patchs
- Injection de code
  - SQL, HTML