Chapitre 4 : Sécurité de l'architecture et des couches basses

(sécurité et parallélisme)

Plan

- Sécurisation de l'architecture
- Contrôle d'accès
- Sécurité des couches basses
  - Couche liaison de données
  - Accès VPN
  - Accès sans-fil
- Annexes

1. Sécurisation de l'architecture

- Sécurité des architectures
- Pare-feu
- Proxy
- NAT
- DMZ
- IDS

Sécurité des architectures

- Sécurité des architectures
  - spécifique à chaque architecture
  - peu de standards
  - souvent insuffisante
- Plusieurs niveaux
  - sécurité des locaux
  - sécurité réseau
  - sécurité des échanges

Sécurité des architectures

- Sécurité des locaux
  - souvent négligée
  - contrôle d'accès nécessaire
- Sécurité réseau
  - couches OSI : physique, liaison de données, réseau, transport
  - solutions souvent implémentées dans le noyau

Sécurité des architectures

- Sécurité des échanges
  - couches supérieures
  - souvent facile et rapide à déployer
  - solutions souvent implémentées au niveau utilisateur

Classification des solutions

- Classification des solutions
  - solutions d'extension
  - solutions transparentes
  - solutions de signalement
  - solutions de traitement local

Classification des solutions

- Solutions d'extension
  - ajouter de nouvelles fonctionnalités aux protocoles
  - problèmes d'interopérabilité
  - exemple : DNSSec
- Solutions transparentes
  - insertion entre deux protocoles
  - pas de modification des protocoles adjacents
  - exemples : SSL/TLS, SSH

Classification des solutions

- Solutions de signalement
  - agissent au sein d'une même couche
  - encapsulation par des protocoles de même niveau (plutôt que d'encapsuler par des protocoles de niveau inférieur)
  - exemple : IPSec
- Solutions de traitement local
  - plupart des solutions déployées
  - pas de problèmes d'interopérabilité
  - exemple : pare-feu, antivirus, IDS

Pare-feu

- Pare-feu
  - équipement permettant de filtrer des paquets
  - règles de filtrage prédéfinies
- Politiques de sécurité
  - internes à l'entreprise
  - externes à l'entreprise

Pare-feu

- Règle par défaut
  - autoriser implicitement : peu sécurisé
  - refuser implicitement : paramétrage contraignant
- Examen des règles
  - examen séquentiel des règles
  - application de la première règle qui coincide

Pare-feu : avantages

- Transparent
- Filtrage à différents niveaux
  - MAC, IP
  - données applicatives
  - par groupe d'utilisateurs
- Capable de gérer des réseaux complexes (NAT, DMZ, VPN)
- Gestion centralisée : simple + possibilité d'audit

Pare-feu : inconvénients

- Cible des attaques
- Contrôle nécessaire de chaque protocole (MAC, IP, HTTP, HTTPS, SQL, ...)
- Nécessite la compréhension des règles de filtrage et de leur ordre d'application

Pare-feu

- Modes de fonctionnement
  - sans état *(stateless)* : chaque paquet est traité indépendemment
  - à état : pour chaque protocole, le pare-feu sauvegarde un état
- Pare-feu sans état
  - filtrage sommaire
- Pare-feu avec état
  - nécessite une machine plus puissante

Pare-feu et ACL

- Fonctionnement d'un pare-feu
  - analyse les entêtes de chaque paquet échangé entre deux machines situées de chaque côté du pare-feu
  - utilise des ACL
- ACL = *Access Control List*
  - IP source, port source, IP destination, port destination
  - TCP (création), TCP (communication) ou UDP
  - autorisation ou refus

Pare-feu et ACL

- IP source et IP destination : masque
- Port source et port destination : *n*, >*n*, liste
- Action
  - autoriser
  - refuser
  - journaliser

Ports fréquents

- Ports fréquents
  - DNS (53)
  - HTTP (80, 8000, 8080) et HTTPS (443)
  - FTP (20 et 21) et TFTP (69)
  - SMTP (25), POP3 (110) et IMAP (143)
  - X (6000 à 6063), RIP (520), NFS (2049), LPD (Line Printer Daemon, 515)

Exemple de pare-feu

- Exemple de spécification
  - r1 - accept from 192.168.1.3:* to 193.49.118.1:25
  - r2 - accept from 192.168.1.0/24:* to *:80
  - r3 - deny from *:* to *:*

Exemple de pare-feu

- Exemple Cisco (simplifié)
  - deny ip 192.168.1.0 0.0.0.255
  - permit tcp any any established
  - permit tcp any host 192.168.1.3 eq smtp
  - permit tcp any host 192.168.1.3 eq dns
  - permit udp any host 192.168.1.3 eq dns
  - deny tcp any any range 6000 6063
  - permit tcp any 20 any gt 1024
  - permit icmp any any

Pare-feu : problèmes

- Problèmes
  - pas d'autentification
  - pas de confidentialité
  - pas de prise en compte des connexions externes
    - accès au réseau qui contourne le pare-feu
    - supports de stockage externes
- Remarques
  - surveiller régulièrement les journaux
  - modifier les règles en fonction des journaux

Proxy

- Proxy = équipement mandataire
  - équipement côté client, relayant (et modifiant) des requêtes entre un client et un serveur
  - utilisation : filtrage, cache, journalisation, anonymat
- Types de proxys
  - proxy générique (ou proxy transparent) ≠ proxy anonymiseur
  - tunnel (ou passerelle) = ne modifie pas les requêtes
  - proxy ouvert
  - reverse proxy

Reverse proxy

- Reverse proxy
  - équipement côté serveur, relayant (et modifiant) des requêtes entre un client et un serveur
  - utilisation : frontal, mémoire cache, équilibrage de charge, contrôle d'accès, compression de contenu

Proxy

- Protocoles concernés généralement
  - HTTP
  - FTP
  - SSH
  - SMTP

Proxy

- Aspects de sécurité
  - anonymat
  - application de politiques de sécurité (contrôle d'accès)
  - journal de l'utilisation
  - examen du contenu entrant (anti-virus, anti-spam) et sortant (fuite d'information)
- Inconvénients
  - contournement de politiques de sécurité

NAT

- Définition : translation d'adresses
  - fonctionnement : principe, table de correspondance
- Avantages
  - adressage interne indépendant de l'adressage externe (flexibilité et masquage de l'architecture)
- Inconvénients
  - modification des sommes de contrôle (IP, TCP)

NAT + PAT

- Définition : translation d'adresses et de ports
  - problème du nombre d'adresses limité
  - fonctionnement : principe, table de correspondance
  - exemple d'utilisation : client interne accédant à un serveur externe
  - mascarade : l'adresse de sortie est l'adresse du routeur

NAT + PAT

- Problème : client externe accédant à un serveur interne
- Solution : configuration manuelle de certaines redirections
- Adresses privées
  - 10.0.0.0 / 8
  - 172.16.0.0 / 12
  - 192.168.0.0 / 16

NAT + PAT

- Avantages
  - pas besoin de beaucoup d'adresses publiques
- Inconvénients
  - initiation par le client seulement
  - le client ne connait pas son adresse IP (problèmes avec certains protocoles comme FTP)

DMZ

- Description de la DMZ
- Buts
  - segmenter le réseau
  - sécurité des parties internes indépendante de la sécurité des parties externes
- DMZ *collapse*

Netfilter

- Netfilter
  - pare-feu logiciel sous Linux
  - permet de gérer le filtrage et le NAT
- (voir feuille supplémentaire)

IDS

- IDS = Intrusion Detection System
  - composant passif
  - complémentaire aux parefeux
- Objectif : détecter les comportements non conformes, les intrusions et les attaques
- NIDS = Network IDS
- HIDS = Host IDS

NIDS

- Mécanisme
  - surveillance du trafic
- Localisation
  - point clef de l'architecture

HIDS

- Mécanisme
  - surveillance des logs d'erreur, des logs d'audit, des droits et des ressources utilisées
- Localisation
  - sur chaque système surveillé

Méthodes de détection

- Détection basées sur des signatures
  - détection de schémas d'attaques connues
  - exemple : attaque des "grands paquets ICMP" sur le parefeu "BlackIce Defender"
- Détection basées sur des anomalies de comportement
  - comparaison du comportement habituel avec le comportement actuel
  - exemple : accès à une ressource à une heure inhabituelle

Méthodes de détection

- Détection par tests d'intégrité
  - vérification de l'intégrité des fichiers
  - mise à jour de l'intégrité des fichiers à chaque mise à jour légitime

Inconvénients des IDS

- Production de faux positifs
  - alarme générée pour un comportement légitime
- Production de faux négatifs
  - absence d'alarme générée pour un comportement illégitime
- Pas de détection de toutes les attaques
- Pas d'évitement des intrusions
- Problème de déploiement

IDS logiciel

- Exemple : SNORT
  - logiciel open-source et gratuit
  - IDS à détection basée sur des signatures
  - mise à jour des signatures fréquentes

2. Contrôle d'accès

- AAA = Authentication, Authorization, Accounting
  - autentification
  - autorisation
  - contrôle d'accès
  - traçabilité
- Architecture
  - client-serveur
  - une seule base d'utilisateurs, mais plusieurs serveurs

AAA

- Très utilisé par les fournisseurs d'accès à Internet (généralisable au réseau interne d'une entreprise)
- NAS = Network Access Server
  - point d'accès au réseau
  - plusieurs NAS
- RAS = Remote Access Server
  - politique d'accès centralisée
  - information sur les clients et les droits
  - configure les NAS

RADIUS

- RADIUS = Remote Authentication Dial-In User Service
  - autentification via une base commune
  - exemple : accès à Internet, POP, apache
  - protocole client/serveur basé sur des requêtes/réponses
  - chiffrement des données par une clé prépartagée
  - port UDP 1812

RADIUS

- Serveur RADIUS
  - interroge une base de données externe (LDAP, SQL, comptes utilisateurs)
- Fonctionnement
  - NAS agit comme intermédiaire entre l'utilisateur et le RAS
  - utilisateur effectue une requête (avec login et password)
  - séquence d'access-request et access-challenge
  - termine par access-accept ou access-reject

RADIUS

- Comptabilisation
  - but : journalisation et facturation
- Mécanisme
  - paquet START lors de l'accès
  - paquet STOP lors de la déconnexion ou d'un timeout
- Légalité
  - l'accès à Internet doit être identifié vers un compte bancaire

RADIUS

- Inconvénients
  - protocole UDP
  - pas de sécurisation au niveau transport (nécessité d'utiliser un VPN)
  - pas d'autentification du serveur

3. Sécurité des couches basses

- Couche liaison de données
  - PAP
  - CHAP
  - PPP
  - EAP
- VPN

Couche liaison de données

- Niveau le plus bas pour la sécurité
  - essentiel
- Type multipoint
  - réseau interne
  - Ethernet
- Type point à point
  - connexion externe
  - PPP

PAP et CHAP

- PAP = Password Authentication Protocol
  - envoi d'un couple (login, password) en clair
  - vérification du couple
- CHAP = Challenge Handshake Protocol
  - client envoie une identification
  - serveur envoie un nombre aléatoire N (nonce)
  - client envoie hash(N, secret partagé)
  - serveur vérifie (en utilisant le secret partagé)

PPP

- PPP = Point to Point Protocol
  - protocole de transmission de niveau 2 entre deux hôtes
  - support de PAP et CHAP
- Mécanismes
  - encapsulation de paquets
  - contrôle de la liaison (LCP = Link Control Protocol) : gère la taille des trames et autorise la communication
  - contrôle de la couche réseau (NCP = Network Control Protocol) : négocie les options IP (timeout)

EAP

- EAP = Extensible Authentication Protocol
  - mécanisme d'autentification universel
  - utilisé en point à point ou en sans fil
- Définit des trames ayant un format spécifique (EAP-request, EAP-response, EAP-success, EAP-failure)
- Extensible
  - mécanismes d'autentification prédéfinis (OTP, ...)
  - toute méthode d'autentification peut être intégrée

VPN

- VPN = Virtual Private Networks
- Objectif
  - interconnecter des machines distantes via un réseau existant
  - former un réseau privé de machines distantes
- Exemple
  - succursales d'une entreprise

VPN

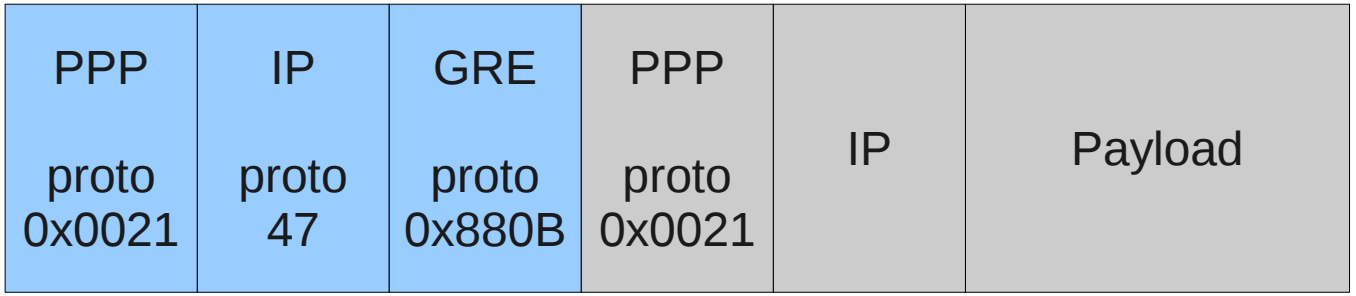
- Interconnexion
  - niveau 2 : par un lien PPP
  - niveau 3 : par un lien IP
- Mécanisme : tunnelling (réalisé par encapsulation)
- Exemples
  - niveau 2 : PPTP, L2F, L2TP
  - niveau 3 : GRE, IPSEC (cf chapitre suivant)

VPN - PPTP

- PPTP = Point-to-Point Tunnelling Protocol
  - RFC 2637, développé par Microsoft
  - protocole client/serveur (et non pas réseau/réseau ou client/réseau)
- Mécanisme
  - signalisation sur le port TCP 1723 (ouverture, fermeture, autentification)
  - protocole de niveau 2 qui encapsule des trames PPP dans des trames IP via GRE

VPN - PPTP

- Avantages
  - supporte MPPE (Microsoft Point-to-Point Encryption)
  - supporte MPPC (Microsoft Point-to-Point Compression)



VPN - L2F

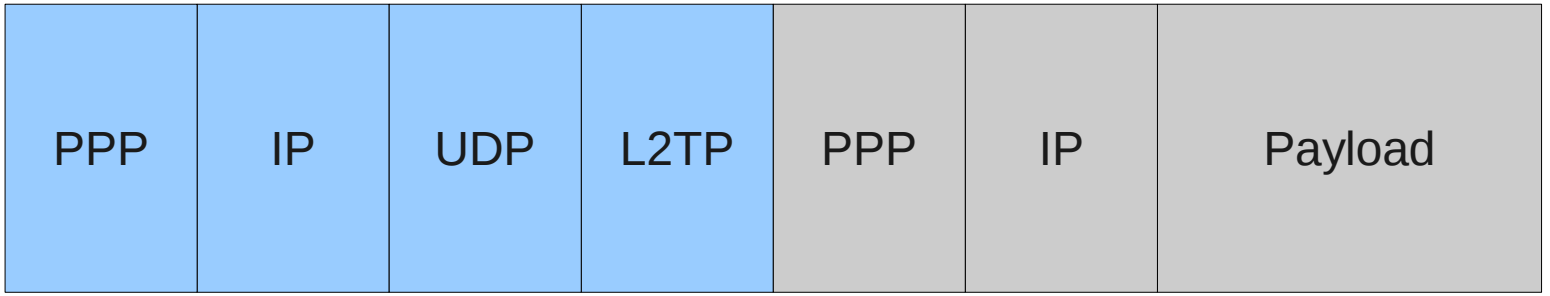
- L2F = Layer Two Forwarding
  - RFC 2341, développé par Cisco
- Mécanisme
  - protocole client/serveur
  - connexion PPP entre le client et le point d'accès au réseau, et tunnel L2F entre le point d'accès au réseau et un serveur distant
- Protocole obsolète

VPN - L2TP

- L2TP = Layer Two Tunnelling Protocol
  - RFC 2661 et RFC 3931, développé par Cisco et Microsoft
  - basé sur PPTP et L2F
- Mécanisme
  - utilise UDP pour encapsuler PPP
  - gestion de la robustesse pour les paquets de contrôle mais pas pour les paquets de données
  - plusieurs VPN peuvent partager le même tunnel

VPN - L2TP

- Avant de communiquer : établissement du tunnel, puis des sessions (= communications)
- Architecture
  - client => LAC (L2TP Access Concentrator) => LNS (L2TP Network Server) => réseau
  - client LAC => LNS => réseau



VPN - L2TP

- Inconvénient
  - pas de confidentialité dans L2TP
- Solution : L2TP/IPSec
  - IPSec crée un canal sécurisé
  - L2TP crée le tunnel sur le canal sécurisé

VPN - GRE

- GRE = Generic Routing Encapsulation
  - RFC 2784, développé par Cisco
- protocole simple
  - définit une enveloppe pour encapsuler un autre protocole
  - sans état

VPN - GRE

- Détection de défaillance du lien
  - si la route vers la destination n'existe pas
  - l'interface qui mène à la destination est stoppée
  - la route pour la destination passe par le tunnel
- Messages keepalive
  - la détection de défaillance précédente ne prend pas en compte les paquets perdus dans le tunnel
  - messages keepalive implémentés de chaque côté du tunnel avec des timers indépendants

4. Annexes

- Netfilter
- (Accès sans-fil)
- (Virus)