

Chapitre 4 : Sécurité de l'architecture et des couches

(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'archite

- 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 les protocoles

Sécurité des architectu

- 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 coûteux
- 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 complets (NAT, DMZ, VPN)
- Gestion centralisée : simple + possible

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 indépendamment
 - 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 d'un 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 : $n, >n$
- 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)
Printer Daemon, 515)

Exemple de pare-feu

- Exemple de spécification
 - r1 - accept from 192.168.1.3:* to 193.49.*
 - 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
 - accès au réseau qui contourne le pare-feu
 - supports de stockage externes
- Remarques
 - surveiller régulièrement les journaux
 - modifier les règles en fonction des jourr

Proxy

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

Reverse proxy

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

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, et sortant (fuite d'information))
- Inconvénients
 - contournement de politiques de sécurité

NAT

- Définition : translation d'adresses
 - fonctionnement : principe, table de corre
- Avantages
 - adressage interne indépendant de l'adr
externe (flexibilité et masquage de l'archi
- Inconvénients
 - modification des sommes de contrôle (l

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 accède à un serveur externe
- mascarade : l'adresse de sortie est l'adresse du routeur

NAT + PAT

- Problème : client externe accédant à serveur interne
- Solution : configuration manuelle de 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 pu
- Inconvénients
 - initiation par le client seulement
 - le client ne connaît pas son adresse IP 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 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 droits et des ressources utilisées
- Localisation
 - sur chaque système surveillé

Méthodes de détection

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

Méthodes de détection

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

Inconvénients des IDS

- Production de faux positifs
 - alarme générée pour un comportement
- Production de faux négatifs
 - absence d'alarme générée pour un comportement illégitime
- Pas de détection de toutes les attaques
- Pas d'évitemment 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 Internet (généralisable au réseau interne 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 privée
 - port UDP 1812

RADIUS

- Serveur RADIUS
 - interroge une base de données externe (MySQL, comptes utilisateurs)
- Fonctionnement
 - NAS agit comme intermédiaire entre l'utilisateur et le RAS
 - utilisateur effectue une requête (avec login, password)
 - séquence d'access-request et access-control
 - 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 timeout
- Legalité
 - l'accès à Internet doit être identifié vers bancaire

RADIUS

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

3. Sécurité des couches ba

- 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 (challenge)
 - 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 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 de la couche réseau

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
 - toute méthode d'autentification peut être utilisée

VPN

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

VPN

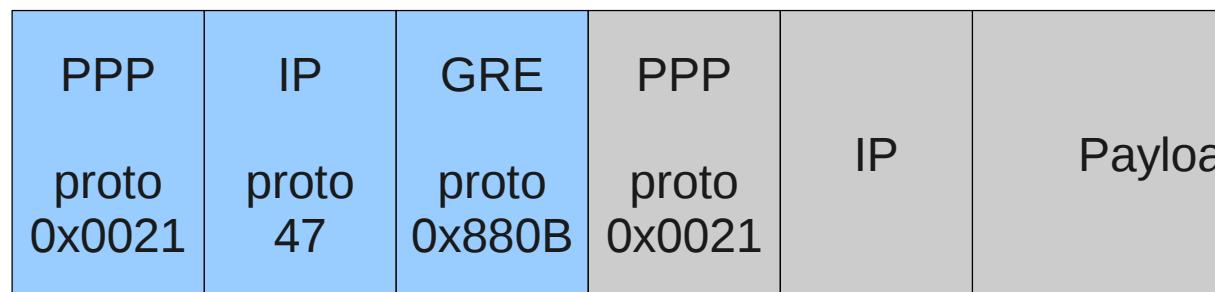
- Interconnexion
 - niveau 2 : par un lien PPP
 - niveau 3 : par un lien IP
- Mécanisme : tunnelling (réalisé par encapsulation)
- Exemples
 - niveau 2 : PPTP, L2F, L2TP
 - niveau 3 : GRE, IPSEC (cf chapitre suivant)

VPN - PPTP

- PPTP = Point-to-Point Tunnelling Protocol
 - RFC 2637, développé par Microsoft
 - protocole client/serveur (et non pas réseau ou client/réseau)
- Mécanisme
 - signalisation sur le port TCP 1723 (ouverture, fermeture, authentification)
 - 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

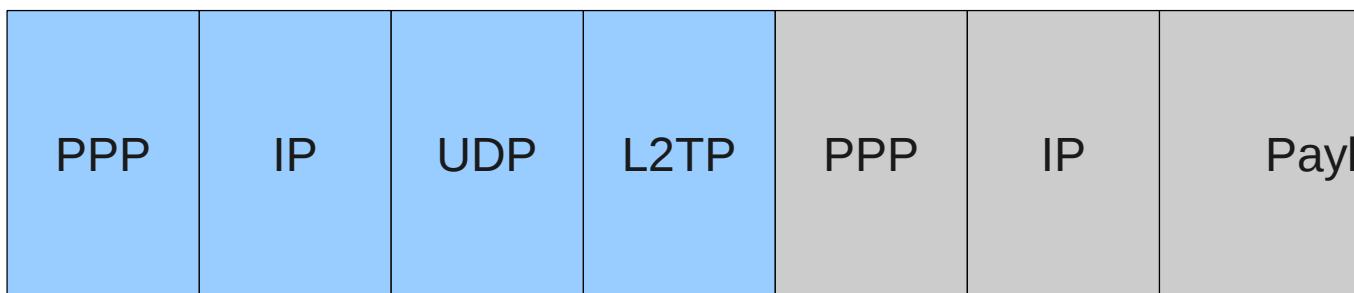
- L2F = Layer Two Forwarding
 - RFC 2341, développé par Cisco
- Mécanisme
 - protocole client/serveur
 - connexion PPP entre le client et le point d'accès réseau, et tunnel L2F entre le point d'accès réseau et un serveur distant
- Protocole obsolète

VPN - L2TP

- L2TP = Layer Two Tunnelling Protocol
 - RFC 2661 et RFC 3931, développé par 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 (= communication)
- Architecture
 - client => LAC (L2TP Access Concentrator / 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 défaillante
 - la route pour la destination passe par le tunnel
- Messages keepalive
 - la détection de défaillance précédente n'en tient pas compte et en tient 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)