Partie 9

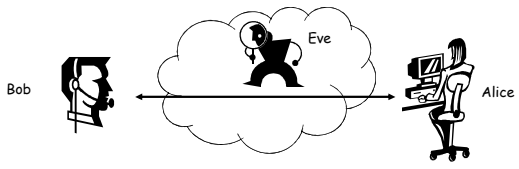
Sécurité

Sécurité - Plan

1. Introduction
2. Cryptographie
3. Exemples

Introduction

- La sécurité réseau a pour but de protéger les données utilisateurs et le fonctionnement du réseau contre les attaques réseaux
- Des attaques réseaux
  - Écoute sur les liaisons réseaux
  - Modification des messages envoyés sur le réseau
  - Déni de service



Services de sécurité réseau

- Identification & autorisation
  - Authentification, signature électronique
- Confidentialité
  - Chiffrement
- Intégrité
  - Checksum (CRC, MIC)

Sécurité - Plan

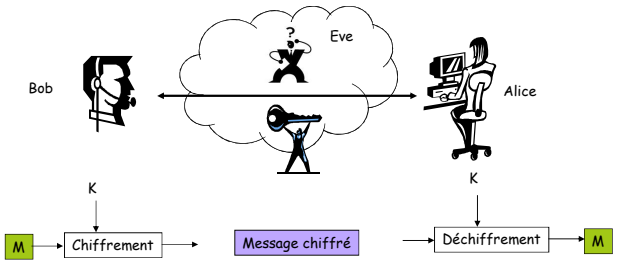
1. Introduction
2. Cryptographie
3. Exemples

Cryptographie

- L' art du secret des données
  - « kruptos » = caché
  - « graphein » = écrire
- Principe
  - Utiliser des fonctions mathématiques paramétrée par une **clé** pour transformer le **text en clair** en **text chiffré** avant d'envoyer le message
- Deux catégories
  - Cryptographie à clé secrète
  - Cryptographie à clé publique

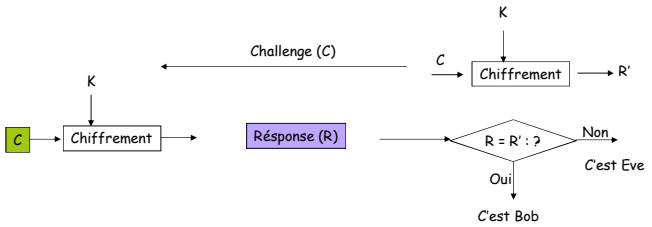
Cryptographie à clé secrète (1)

- Les deux entités de communication partagent la même clé secrète K



Cryptographie à clé secrète (2)

- Authentification

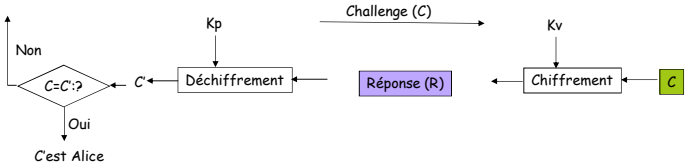


Cryptographie à clé publique (1)

- Chaque entité de communication utilise une paire de clé
  - Clé publique (Kp) pour le chiffrement
  - Clé privée (Kv) pour le déchiffrement

Cryptographie à clé publique (2)

- Authentification
  - Clé privée (Kv) pour le chiffrement
  - Clé publique (Kp) pour le déchiffrement



Sécurité - Plan

1. Introduction
2. Cryptographie
3. Exemples

Securité Wi-Fi

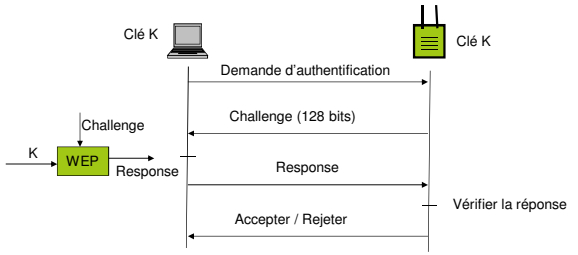
- 1ère génération Wireless Equivalent Privacy (WEP), défini dans le standard 802.11
  - Une seule clé pour l'authentification et le chiffrement
- 2è génération, architecture 802.1x (avec WEP)
  - Deux clés: une pour l'authentification et une pour le chiffrement
- 3è génération, TKIP, WPA
- 4è génération, 802.11i + AES

WiFi sécurité

- Réseau d'accès
  - Service Set ID (SSID) : le nom n'est pas visible
  - Access Control List (ACL) : utilise des listes d'adresses MAC
- Wired Equivalent Privacy (WEP) : mécanisme de chiffrement utilisant l'algorithme RC4
  - Authentification
  - Chiffrement

Authentification avec WEP

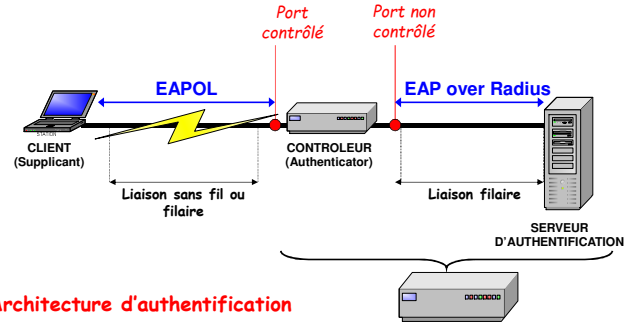
- Le point d'accès accepte seulement les terminaux qui prouvent la connaissance d'une clé secrète partagée entre le point d'accès et le terminal



WiFi sécurité – 2è génération

- IEEE 802.1x ; pour WiFi mais aussi tous les contrôleurs
- Utilisation de EAP (Extensible Authentication Protocol)
- Utilisation d'une authentification de type RADIUS : Remote Authentication Dial in User Service

IEEE 802.1x

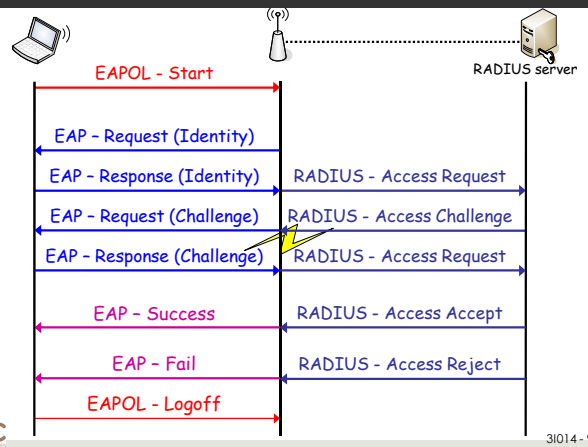


Architecture d'authentification

RADIUS : Remote Authentication Dial in User Service

EAP : Extensible Authentication Protocol

EAPOL/RADIUS



WiFi security – 3rd generation

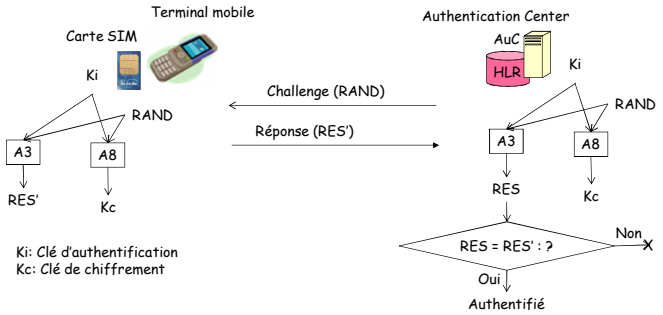
- TKIP : Temporal Key Integrity Protocol
- WPA : Wi-Fi Protected Access
  - Proposition de la WiFi Alliance
  - Basé sur TKIP : modification de la clé toutes les N frames
  - IEEE 802.1x
- Oroblème potentiel : RC4

WiFi sécurité – 4è génération

- Juin 2004 : WPA2
- Utilisation de TKIP et de 802.1x
- Nouvel algorithme de chiffrement: AES
  - L'algorithme RC4 est remplacé par AES

Sécurité GSM (1)

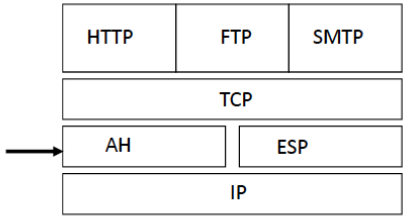
- Authentification



Sécurité GSM (2)

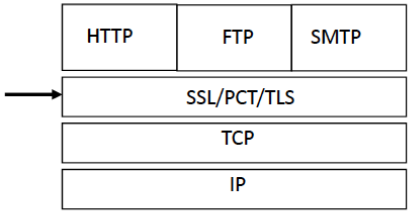
- Chiffrement des appels

Sécurité TCP/IP (1)



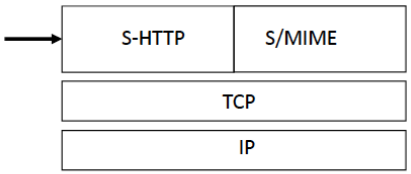
Approche réseau

Sécurité TCP/IP (2)



Approche transport

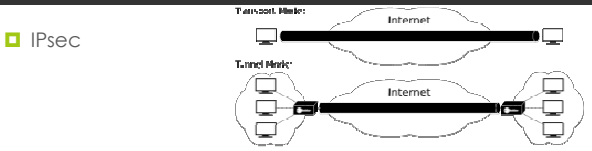
Sécurité TCP/IP (3)



Approche application

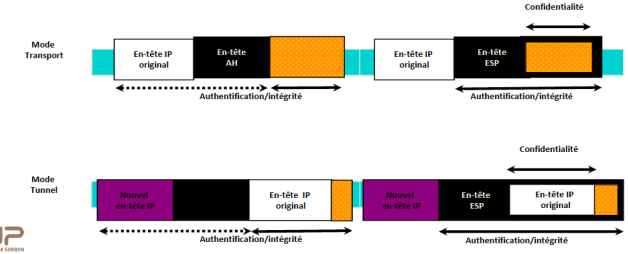
Sécurité TCP/IP (4)

- IPsec



AH
AH -Authentication Header

ESP
ESP - Encapsulating Security Payload



Firewall et DMZ