Comité Réseau des Universités

CRU

# ARREDU

## Considérations de sécurité autour de Radius

C. Claveleira

Réunion de travail ARREDU

14 juin 2005

Renater - Paris

CRU

# Radius : modèle de sécurité

- Sécurité « hop to hop »
- Secret partagé entre partenaires
  - Utilisé pour l'authentification des partenaires et la protection des mots de passe (PAP)

CRU

# Vulnérabilités

- Secret partagé crackable par sniffing
- Access-Request uniquement authentifié par @ IP par défaut ?
- Robustesse du mécanisme de masquage de mot de passe  non prouvée
- => le trafic Radius ne doit pas pouvoir être écouté (vlans dédiés, IPSec,...)

CRU

# Problèmes liés aux mots de passe

- Mots de passe manipulés par chaque serveur/proxy (déballage/remballage)
  - Interception aisée si machine compromise
  - Peuvent apparaître en clair dans les logs si serveur en mode debug
- Acceptable au sein d'un même domaine de gestion ?
- Inacceptable entre domaines différents ?

CRU

# Pb particuliers au sans-fil

- Lien entre poste et borne peu ou pas sécurisé (sauf WPA)
- => besoin de chiffrement au-dessus de la liaison
- 802.1x sujet aux attaques de type man in the middle
- Risque de faux points d'accès (faciles à mettre en oeuvre)

CRU

# Solutions

- EAP
- Chiffrement
- Authentification mutuelle

# EAP

- Cadre générique support de protocoles d'authentification
  - MD5
  - OTP
  - TLS
  - SIM
  - AKA
  - PEAP
  - ...
- Utilisé en 802.1x
- Transporté de façon quasi-transparente par Radius
- => plus de manipulation des mots de passe par les serveurs Radius

CRU

# Protection de l'authentification

- Utilisation de tunnels chiffrés de type TLS
- Transportés de façon transparente via Radius/EAP : TTLS, TLS, PEAP,...
- -> tunnel de bout en bout entre poste (supplicant) et serveur Radius de rattachement
- Authentification du serveur Radius de rattachement par le supplicant
- Authentification mutuelle possible par certificat (TLS)
- => protection de la phase d'authentification (et donc des *credentials*)
- => élimine le risque des points d'accès pirates

CRU

# Protection du lien radio

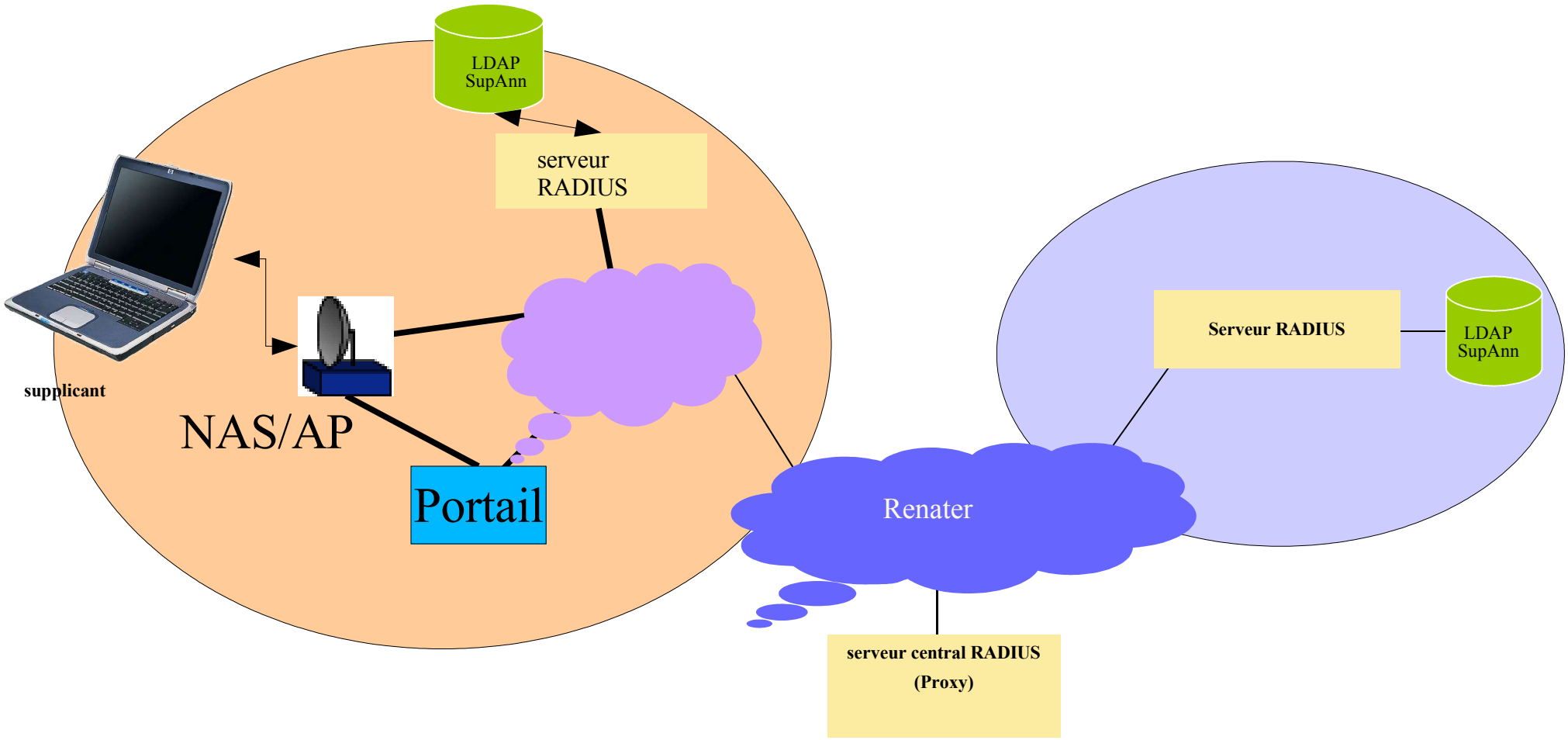
- WEP dynamique (lié à 802.1x) ou WPA
- N'intervient qu'après la phase d'authentification
- Protection des données échangées
- Protection contre attaques MIM/DOS ?

CRU

# Risques des portails captifs Wifi (et web)

- Pas de sécurisation du lien radio -> sniffing et spoofing, MIM
  - >il faut sécuriser la phase d'authentification autrement (https)
  - >il faut sécuriser les échanges de données autrement
- Éléments d'authentification manipulés par le portail (sauf si redirection vers le site d'origine)
- -> comment être sûr qu'ils ne peuvent pas être interceptés, détournés,... ?
-
- Facile de monter un faux portail (même avec certificat) derrière un faux point d'accès

# Flux


LDAP
SupAnn
serveur
RADIUS
supplicant
NAS/AP
Portail
Renater
Serveur RADIUS
LDAP
SupAnn
serveur central RADIUS
(Proxy)
authentification
data
univ-orange.fr
univ-bleue.fr