

La sécurité WiFi, depuis le WEP jusqu'au 802.11i

Alexandre Fernandez

<Alexandre.Fernandez@hsc.fr>

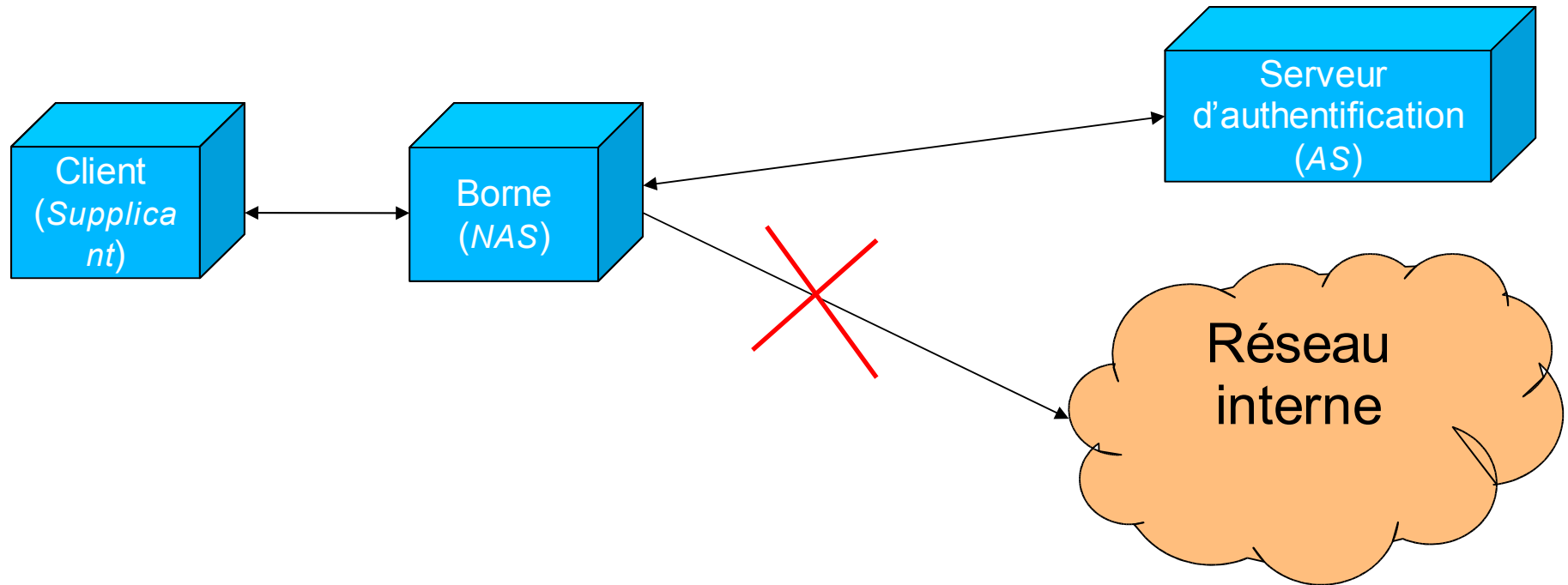
- x **Avantages**

- x Chiffrement
- x Authentification
- x Simplicité

- x **Inconvénients**

- x Secret partagé
- x Secret très partagé
- x Choix du mot de passe
- x Chiffrement RC4
- x Réutilisation du vecteur d'initialisation
- x Administration difficile

Principe 802.1x



- × Pendant la phase d'authentification
 - × La station ne peut accéder qu'au serveur d'authentification
 - × Tous les autres flux sont bloqués par l'AP
- × Après authentification, les flux vers le réseau interne sont permis

- x Avantages
 - x Clé spécifique pour chaque client
 - x → Vraie confidentialité entre client et AP
 - x Renouvellement possible de clés
 - x → Rend plus difficile la cryptanalyse
 - x Usage d'un serveur d'authentification
(*RADIUS ou autre*)
 - x → Administration centralisée

- x Inconvénients
 - x Ecoute du trafic d'authentification
 - x Attaque « *man in the middle* »
 - x Déni de service
 - x Complexité
 - x Besoin d'un serveur d'authentification
 - x Déploiement de certificats
 - x Très nombreuses options possibles

- x Principe
 - x Conçu par la WiFi Alliance
 - x Solution
 - x Pragmatique
 - x Transitoire
 - x Basé sur des briques existantes
 - x 802.1x, EAP, TKIP, RADIUS

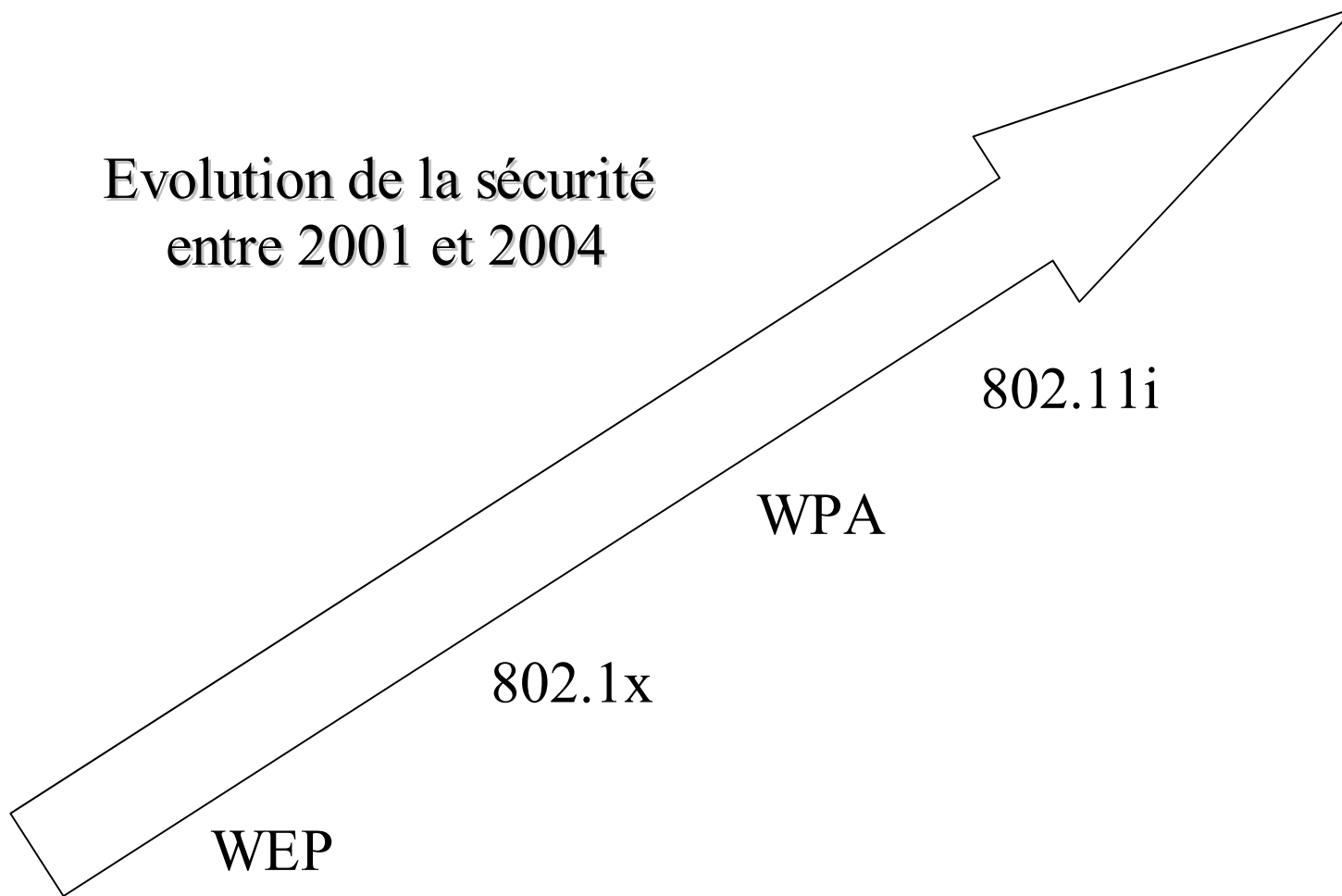
- x Avantages fonctionnels
 - x Compatible avec les équipements actuels
 - x → Mise à jour logicielle
 - x Facile à déployer en environnement SOHO
 - x WPA-PSK avec « *passphrase* »
- x Avantages techniques
 - x Usage de TKIP
 - x L'IV passe de 24 à 48 bits
 - x Usage d'un MIC
 - x Règles de séquençement

- × Inconvénients
 - × TKIP repose toujours sur RC4
 - × Temps de latence lors de la ré authentication lors du passage d'une borne à l'autre
 - × Problème pour les applications en temps réel

- x Principe
 - x Reprend les mêmes mécanismes que WPA
 - x La gestion de la clé est la même que WPA
 - x Utilise AES pour le chiffrement des trames

- x Avantages
 - x Usage d'AES
- x Inconvénients
 - x Achat de nouveau matériel souvent nécessaire
 - x Une simple mise à jour logicielle ne suffit pas

Evolution de la sécurité
entre 2001 et 2004



- x Tendance sur les produits d'aujourd'hui
 - x Power over Ethernet
 - x Transfert de l'intelligence de la borne vers le commutateur
 - x Cartographie des bornes
 - x Administration centralisée
 - x Attitude active et automatique face aux attaques

- x La normalisation arrive enfin à maturité
- x Les produits dimensionnés pour l'entreprise
 - x Conformes avec les normes en vigueur
 - x Fournissant des services adaptés aux besoins des entreprises
- x Ne jamais oublier
 - x Des failles dans les implémentations sont toujours possibles
 - x Des failles dans la configuration sont très souvent présentes
- x Prochain défi : La qualité de service