WEP

Quelques aspects de la sécurité

- Confidentialité
  - Les hackers ne peuvent pas comprendre nos messages
- Intégrité
  - Les hackers ne peuvent pas changer nos messages
- Authentification
  - Les hackers ne peuvent pas utiliser notre réseau
- Protection contre les doublons
  - Les hackeurs ne peuvent pas réinjecter nos messages

Confindentialité

- Comment pourrait-on faire pour que nos messages ne soient pas compris ?

Confidentialité

⊕ Ou exclusif

Données: 1 0 0 0 1 0 1 1 0 1 1

⊕

Séquence secrète: 0 1 1 0 1 0 0 1 1 0 1

Séquence envoyée: 1 1 1 0 0 0 1 0 1 1 0

⊕

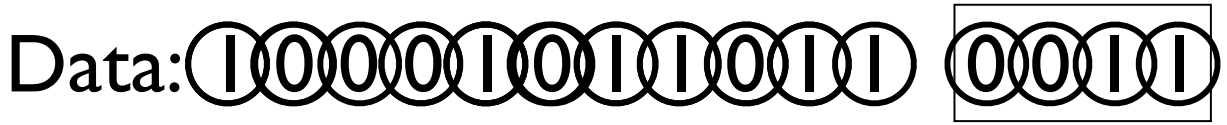
Séquence secrète: 0 1 1 0 1 0 0 1 1 0 1

Données: 1 0 0 0 1 0 1 1 0 1 1

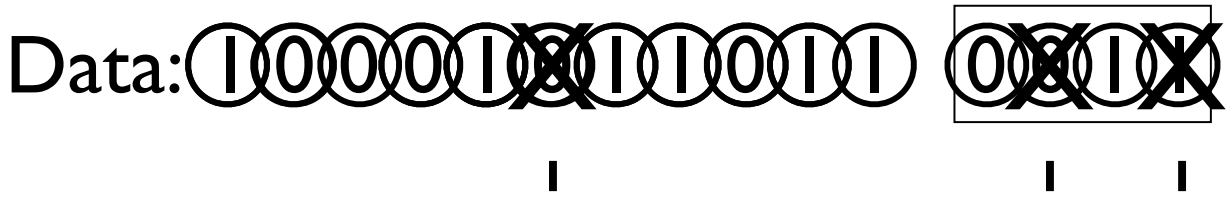
Intégrité

- Comment pourrait-on faire pour détecter qu'un message a été changé en cours de route ?

Intégrité



... séquence reçue



Authentification

- Comment pourrait-on empécher que des utilisateurs non-autorisés utilisent notre réseau ?

Protection contre doublons

- Comment pourrait-on reconnaître une trame qui a été réinjectée par un hacker ?

Sécurité dans WiFi avant WPA

WEP - Wired Equivalent Privacy
(Equivalent à la sécurité câblée)

Sécurité avant WPA

WEP (Wired Equivalent Privacy)

- Confidentialité
  - Chiffrement des données
- Intégrité
  - Integrity Check Value (ICV)
- Authentification
  - Optionnelle: Shared Key Authentication
- Protection contre les doublons
  - Aucune

WEP

A.K.A. ICV

- Calculer le CRC sur le corps de la trame
- Ajouter le CRC au corps de la trame
- Enchaîner l'IV de 24-bit avec la clé partagée (40 bit ou 104 bit) pour créer la graine RC4
- Générer une séquence pseudo-aléatoire de la bonne longueur
- Calculer XOR de la séquence pseudo-aléatoire avec la trame+ICV
- Ajouter l'IV au début de la trame
- Envoyer comme une trame de données normale

Clé partagée

- Séquence “secrete” de 40 bits ou 104 bits
- Connue par l’AP et les STAs authorisées
- Peut être dérivée à partir d’un mot de passe
- L’algorithme de conversion pour passer du mot de passe —— clé es proprietaire

Initialization Vector

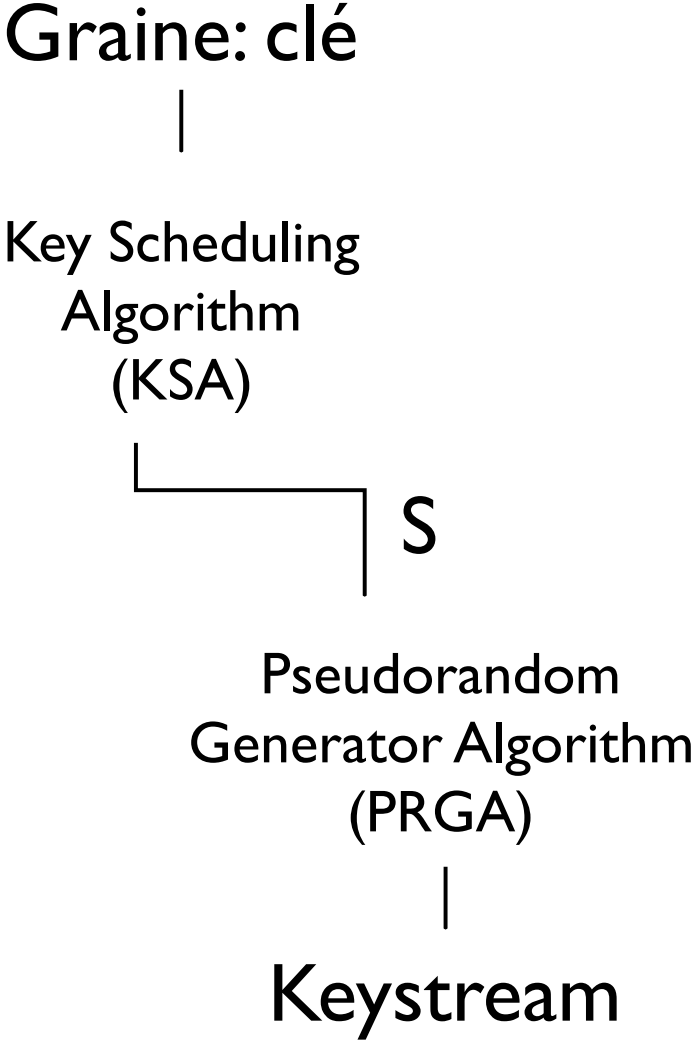
Initialization Vector (IV) - 24 bits

2^{24} = 16’777’216 combinaisons différentes

Censé faire chaque clé de chiffrement “unique”

RC4

- Chiffrement de flux
- Ron Rivest Cipher 4
- Créé en 1987
- “Fui” en 1994
- Extrêmement simple et rapide
- Vulnérable à la réutilisation du flux de chiffrement (Keystream)



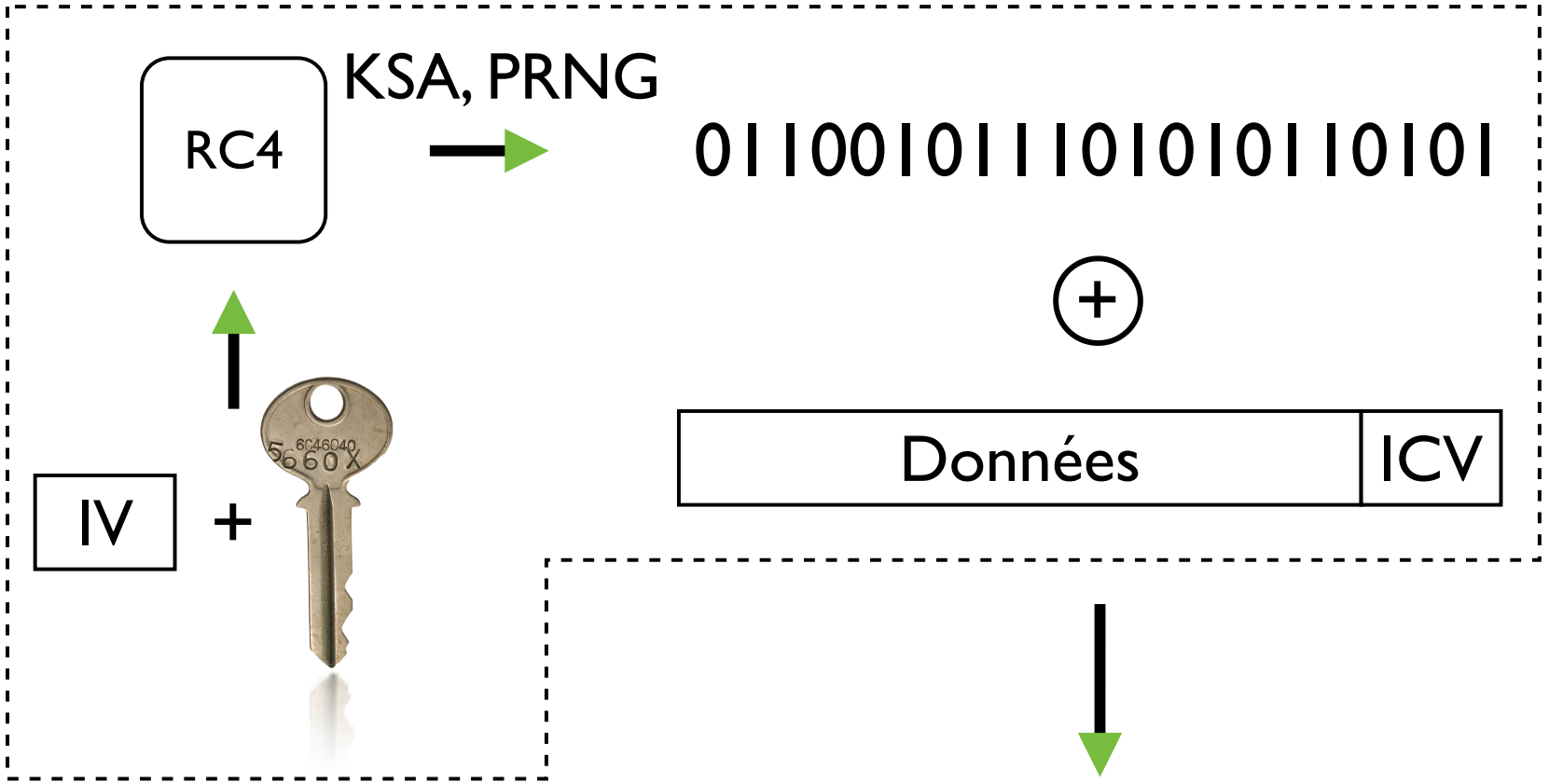
WEP et l'intégrité

Integrity Check Value

- L'intégrité des données est assurée par le'ICV
- CRC "normal" de 32-bit
- Pas vraiment un test d'intégrité
- ... plus sur ceci un peu plus tard...

WEP et la confidentialité

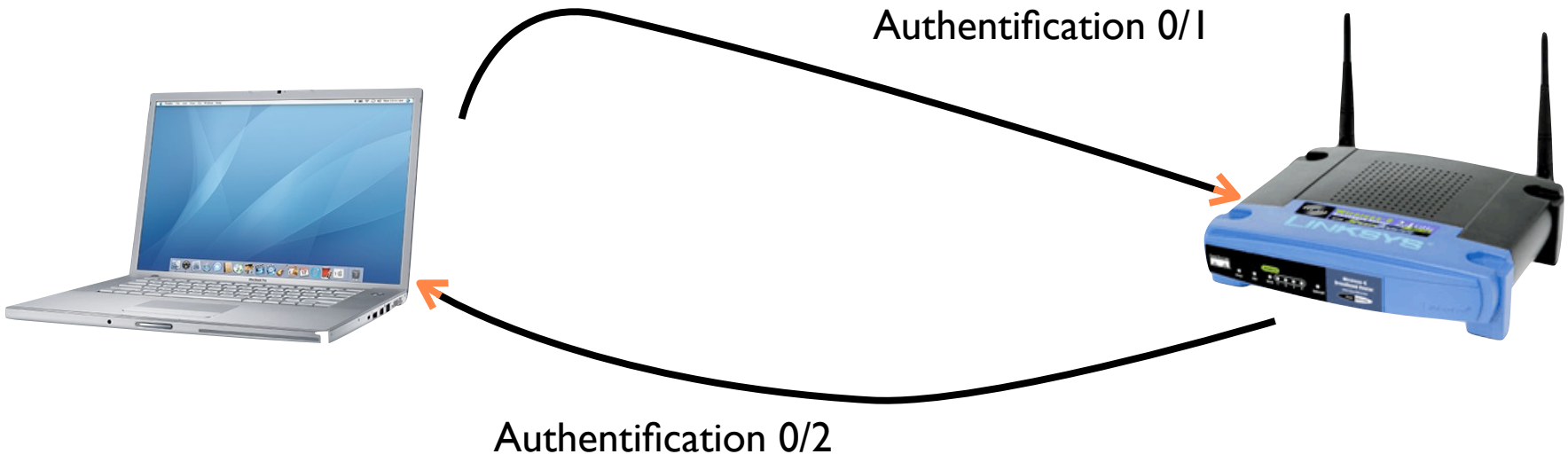
L'algorithme WEP



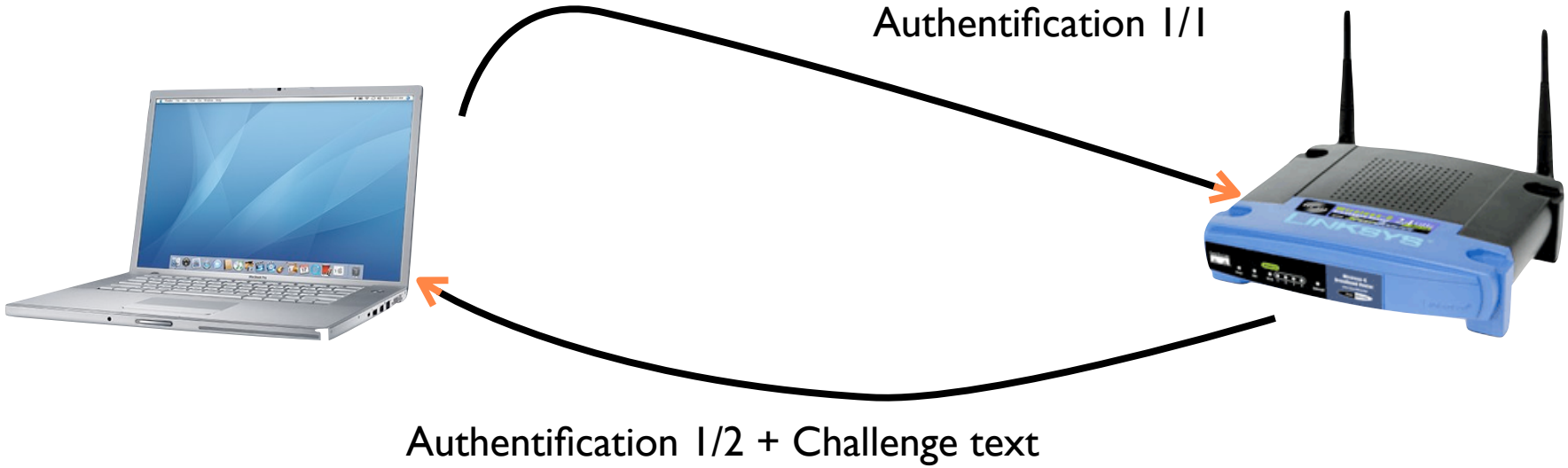
MAC Header	IV Header	Corps de la trame	ICV	CRC

WEP et l'authentification

Système ouvert

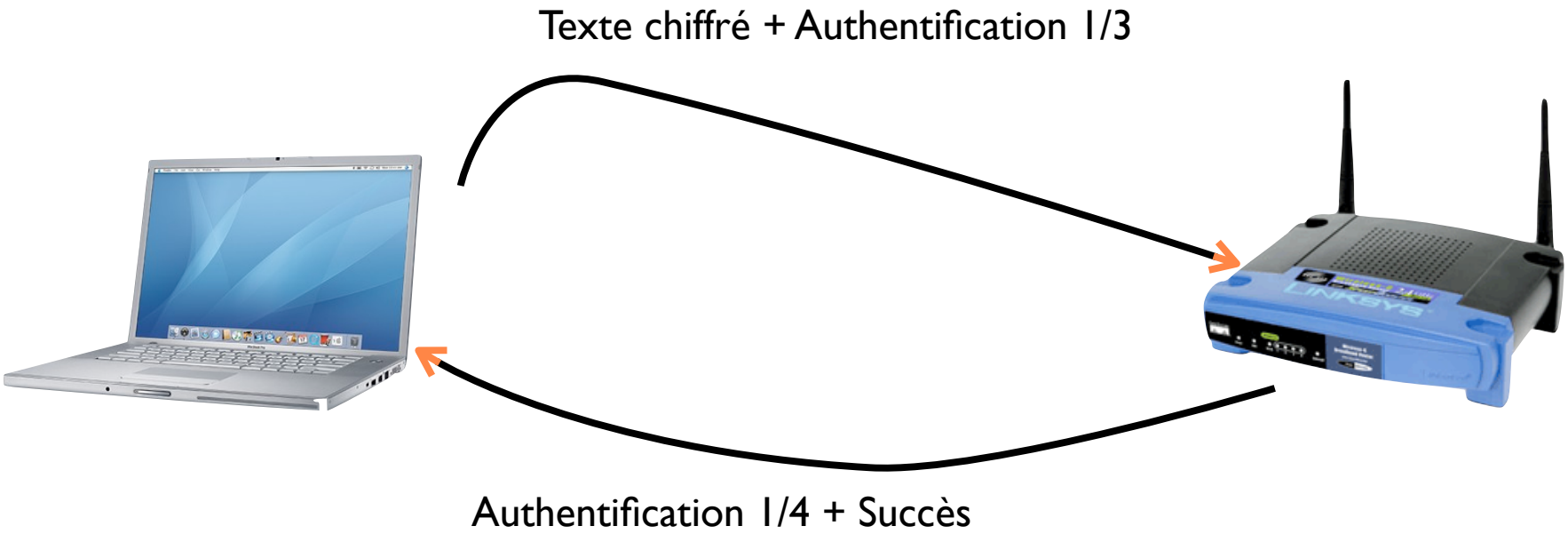


Clé partagée



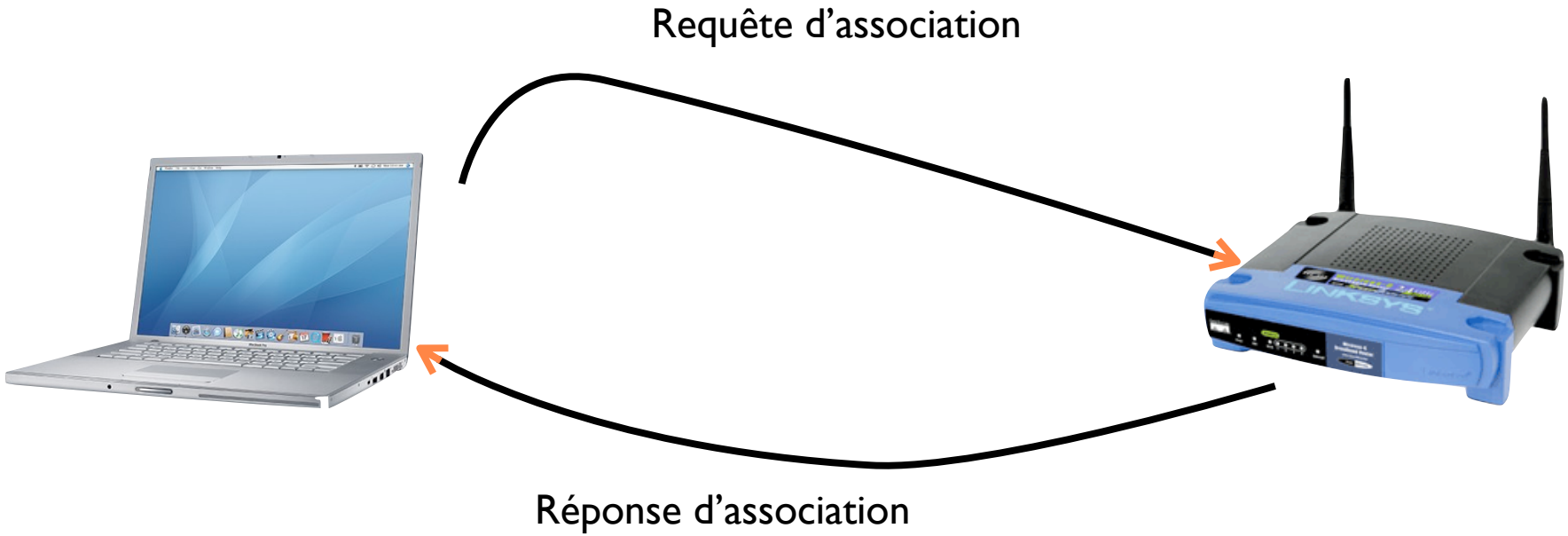
Clé partagée

Comment la STA sait-elle qu'elle peut faire confiance à l'AP ?



Association

La STA est maintenant authentifiée
mais elle n'est pas encore associée



Pourquoi le WEP a-t-il échoué ?

Confidentialité

- Non conçu ni supervisé par des cryptographes
- Mauvais choix d'algorithme de chiffrement
  - Le chiffrement RC4 est faible
- La partie secrète de la clé est la même pour tout le monde
- La partie envoyée en clair (IV) a 24 bits (la clé est réutilisée après 2^{24} trames)
- Les STAs utilisent le même IV quand elles commencent à transmettre
- Il existe de méthodes qui permettent de découvrir la clé WEP à partir d'un certain nombre de trames

Intégrité

- Le contrôle d'intégrité n'est pas cryptographiquement sûr
  - L'utilisation du CRC est "ok" pour des erreurs aléatoires mais non pas pour les erreurs délibérées
- Il est possible de modifier des messages sans être détecté (changer des données et ICV)

Authentification

- Optionnelle
- Système ouvert - défaut
- Aucune authentification bidirectionnelle.
  Seulement la STA est authentifiée
- Le challenge dans l'authentification à clé partagée est envoyé en clair
  - Exposition dangereuse à des attaques connus

Doublons

- Aucune protection contre les doublons

Distribution de clés

- Aucune méthode centralisée

Pas du tout “équivalent à la securité câblée” !

- Les gens qui ont entendu parler des vulnérabilités WEP les regardent encore comme “théoriques”
  - Les premières méthodes de cracking exigeaient des quantités impraticables de données
- Le cracking WEP de dernière génération est significativement plus agressif, plus rapide et beaucoup plus facile...