Les mécanismes de sécurité du Wireless LAN

Philippe Oechslin

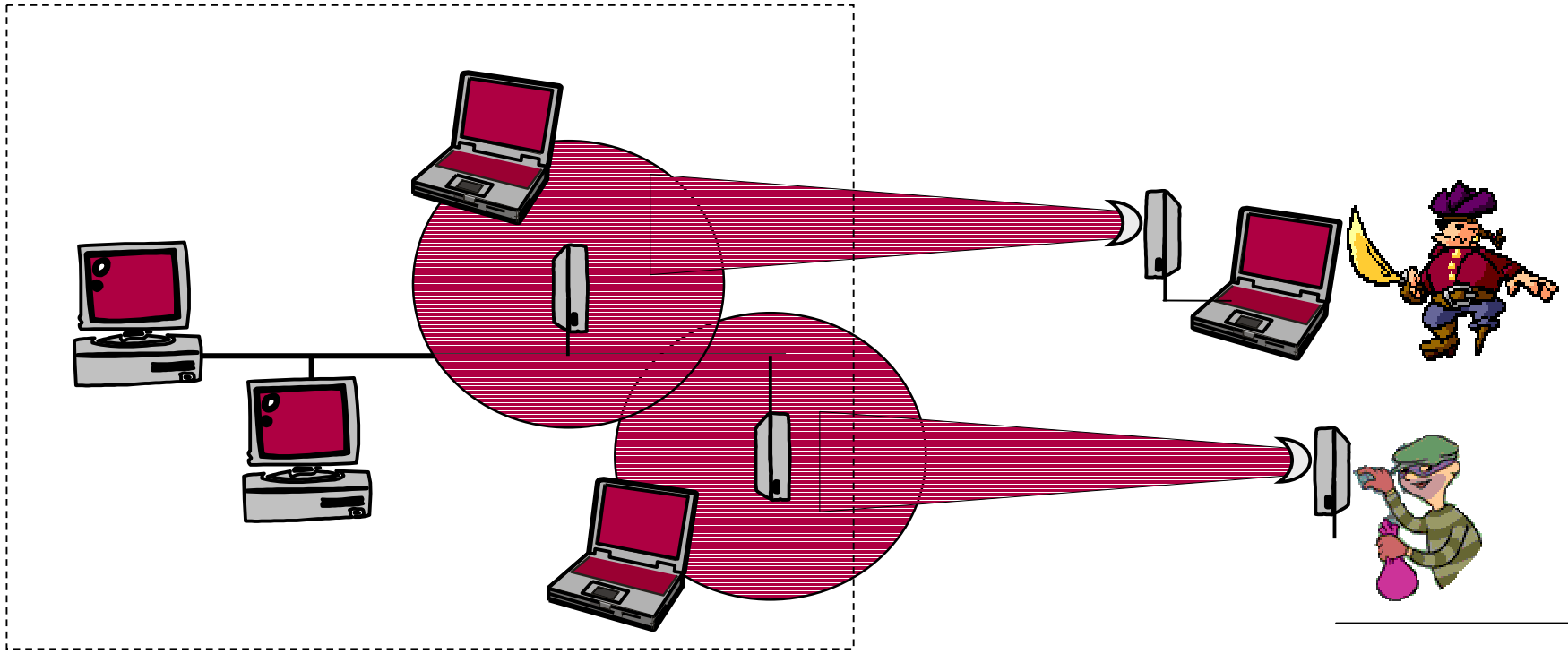
Laboratoire de Sécurité et de Cryptographie

Ecole Polytechnique Fédérale de Lausanne

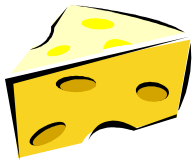
philippe.oechslin@epfl.ch

Tout le monde sait…

- que le Wireless LAN n'est pas sûr
- Mais pourquoi? Et comment peut-on se protéger?

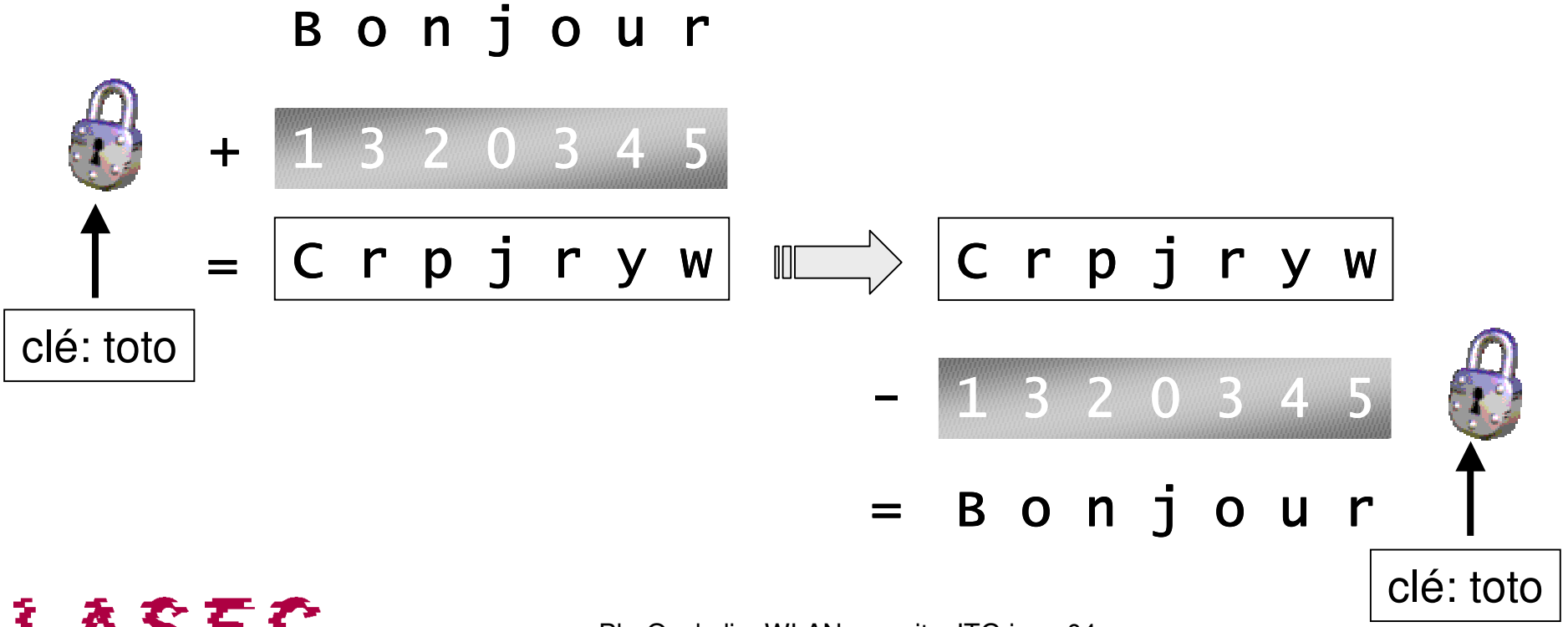


Le WEP, source du problème

- Le WEP (Wired Equivalent Privacy) est le mécanisme original qui devait protéger les WLAN 802.11
- Développé par des non-spécialistes en comité fermé
  - Résultat: 
- Problèmes majeurs
  - Authentification faible: **usurpation d'identité**
  - Contrôle d'intégrité faible: **modification, injection, reroutage des données**
  - Chiffrement faible: **décryptage des données, récupération de la clé unique**

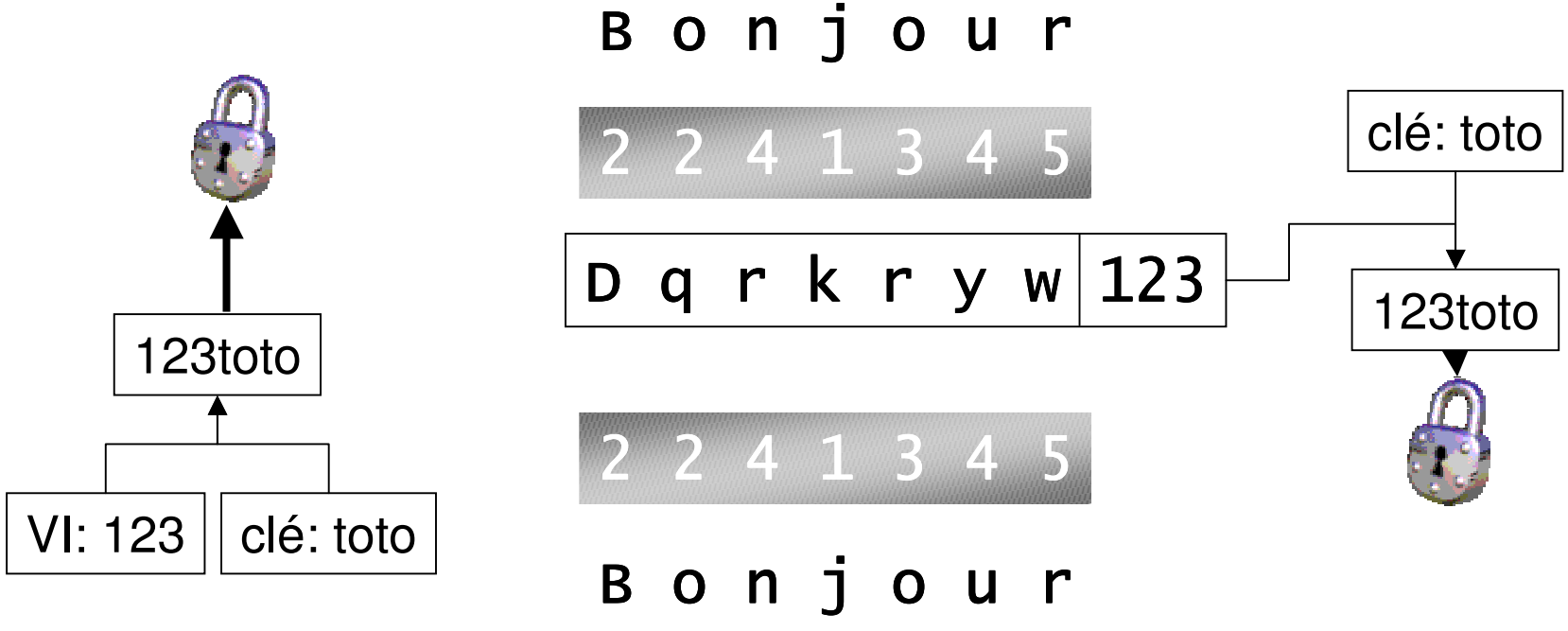
Fonctionnement de RC4

- Le chiffrement de WEP est basé sur RC4
  - RC4 est sûr, il est utilisé par exemple pour le e-banking
- C'est un algorithme de chiffrement par flot (stream cipher)



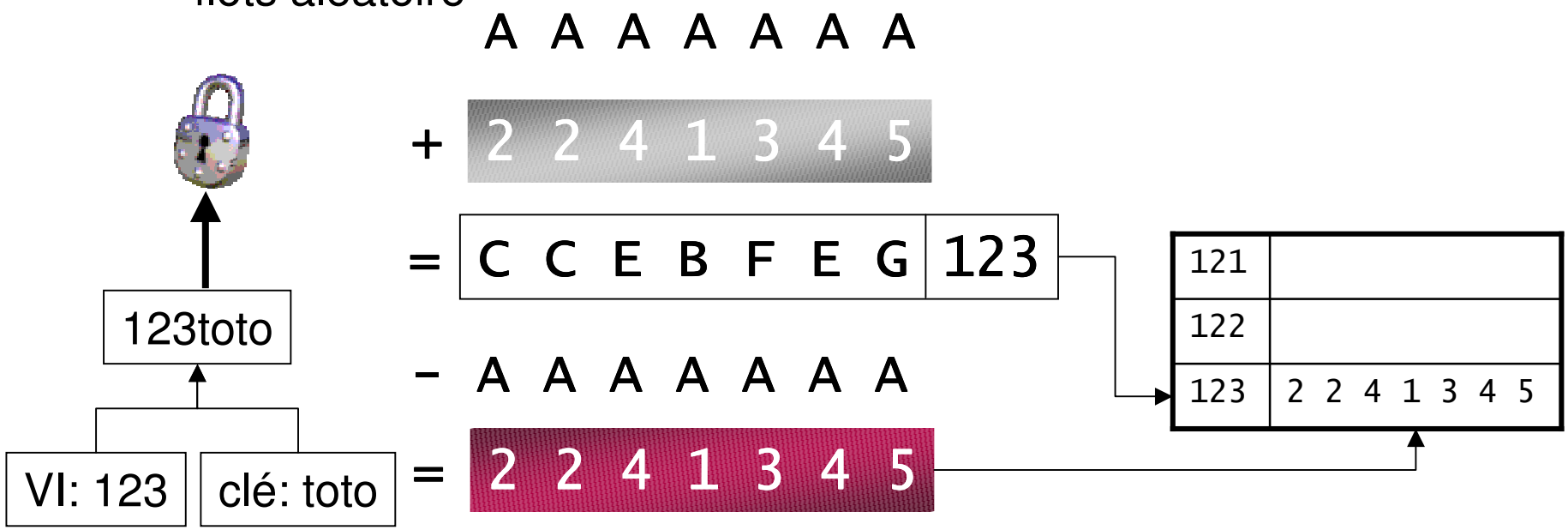
Vecteur d'initialisation

- Pour éviter de toujours générer le même flot aléatoire, on ajoute un vecteur d'initialisation (VI) à la clé
  - On transmet le VI en clair pour permettre le déchiffrement



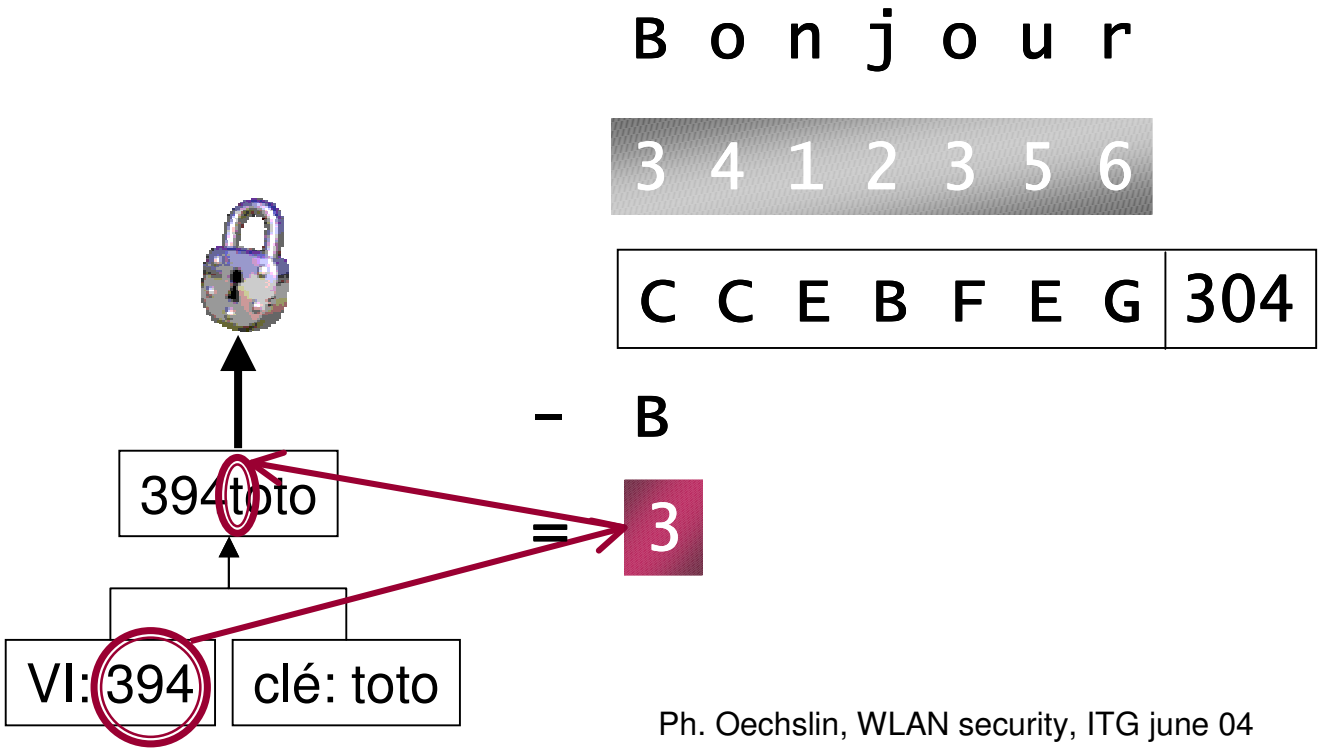
Faiblesses du WEP (1)

- Il n'y a « que » 16 mio de vecteurs d'initialisation
  - Ils se répètent après une journée de trafic
  - Si on connaît des textes clairs, on peut établir un dictionnaire des flots aléatoire



Faibless du WEP (2)

- Le vecteur d'initialisation représente les premiers bytes de la clé RC4
  - si on connaît les premiers bytes de la clé, on peut trouver le prochain byte à partir du premier byte du flot aléatoire (IV faibles)
  - On trouve le premier octet clé avec un million de paquets
  - Récupération de la clé complète en temps linéaire!



Faiblesses du WEP (3)

- Le code correcteur est linéaire crc(M1) +crc(M2) = crc(M1+M2)

```
  Bonjour  crc(Bonjour)
+     9070  crc(   9070)
------------------------
= Bonsoar  crc(Bonsoar)
```

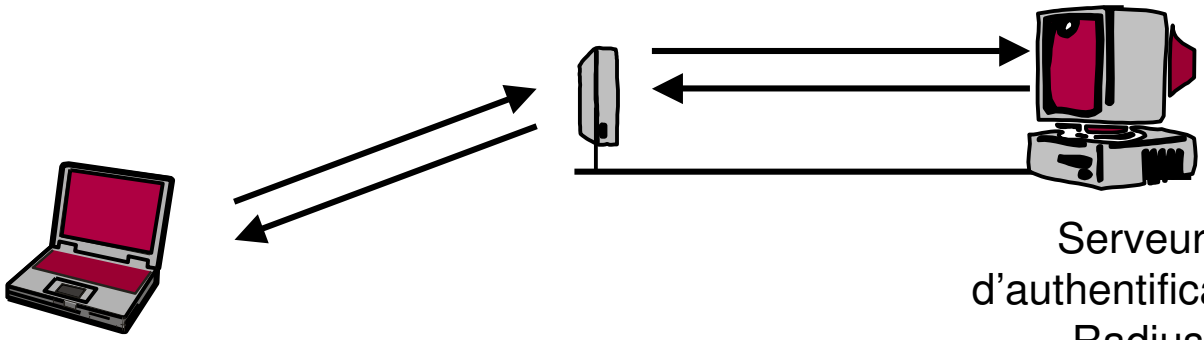
```
  B o n j o u r, crc(Bonjour)
+ 2 2 4 1 3 4 5   3
------------------------
= D q r k r y w   crc(Bonjour)+3
+           9 0 7 0 crc(   9070)
------------------------
= D q r k r y w   crc(Bonjour)+3
                  +crc(   9070)

- 2 2 4 1 3 4 5   3
------------------------
= B o n s o a r   crc(Bonsoar)
```

Faiblesses du WEP (suite & fin)

- Grâce au CRC linéaire, un pirate peut modifier l'adresse de destination d'un paquet chiffré:
  - Le paquet sera déchiffré et envoyé par Internet chez le pirate!
- La clé WEP est la même pour tous les utilisateurs du WLAN
  - Impossible de coordonner la mise à jour de la clé
- Les faiblesses ne sont pas dues à RC4. Dans TLS:
  - on utilise des clés de session uniques
  - on ne recommence pas le flux aléatoire à chaque transmission (pas de VI)
  - on jette les premiers bytes générés par RC4 (pas de récupération de la clé)
  - on utilise on code de détection d'erreur non-linéaire
- On aurait pu s'en inspirer pour le WEP…

Solutions

- WEP+
  - Ne pas générer de VI faibles
    - Evite la récupération de la clé
- 802.1x (Windows XP SP1)
  - Protocole d'authentification extensible EAP
  - Permet d'authentifier les utilisateurs avec un serveur Radius
  - Ils doivent taper leur mot de passe ou posséder un certificat pour avoir accès au réseau
    - On peut gérer l'accès de chaque utilisateur



Serveur d'authentification Radius

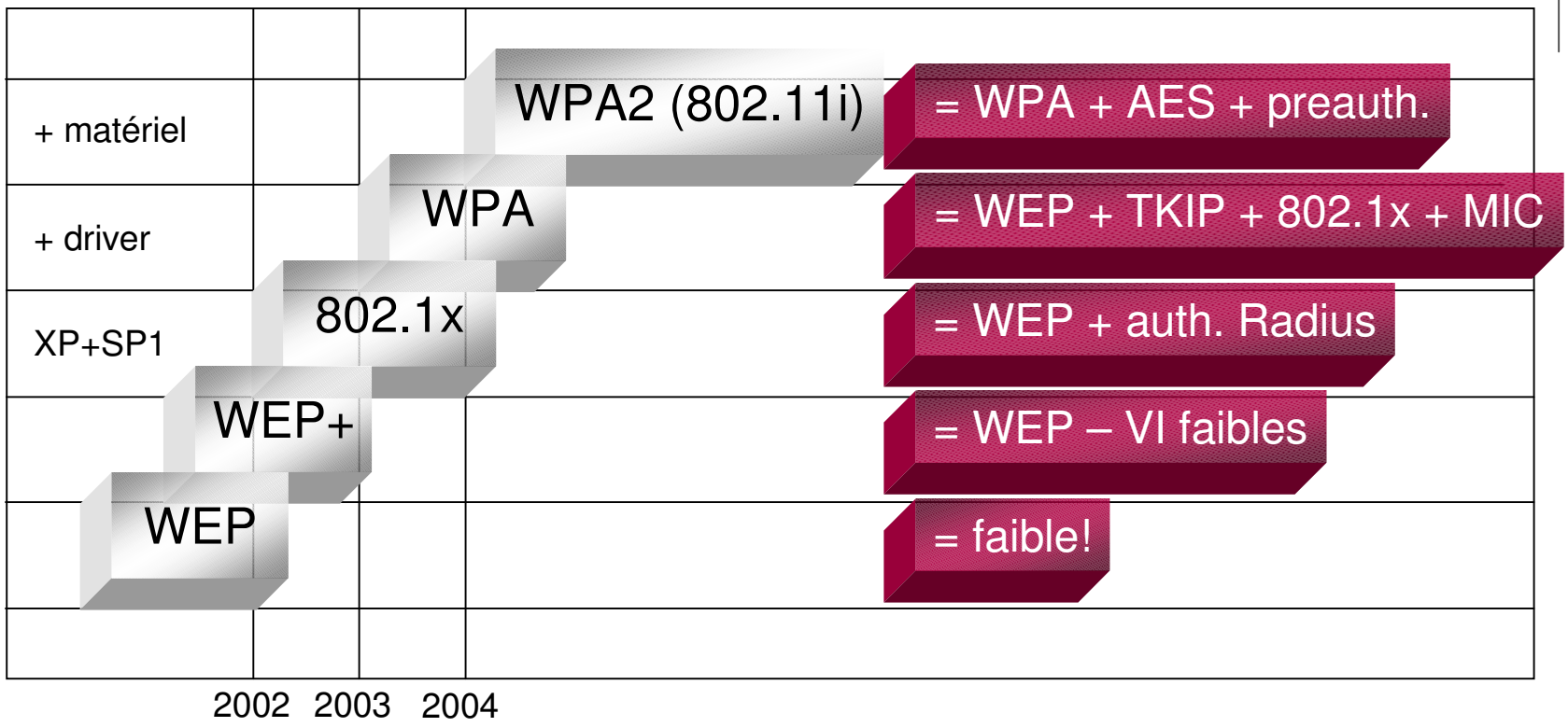
WPA (WiFi Protected Access, 2003)

- Authentification: EAP (802.1x)
- Chiffrement: TKIP (temporal key integrity protocol)
  - Clé maîtresse de 256 bits
  - Utilisation d'une clé différente pour chaque station
  - Nouvelle clé WEP de 128 bits dérivée tous les 10'000 paquets
  - VI de 48 bits uniques (compteur)
- Contrôle d'intégrité: Michael (MIC)
  - Code de contrôle d'intégrité cryptographique avec une clé de 64 bits
- Compatibilité avec le matériel existant

Le futur: WPA2 (802.11i)

- Authentification: EAP (802.1x)
  - Idem WPA
- TKIP et Michael sont supportés
  - Compatibilité WPA
- Préauthentification
  - Authentifie le trafic de contrôle (association)
    - Évite les dénis de service
- Chiffrement par AES
  - Remplace TKIP et Michael
  - Changement de hardware nécessaire

Résumé


+ matériel
+ driver
XP+SP1
2002
2003
2004
WEP
WEP+
802.1x
WPA
WPA2 (802.11i)
= faible!
= WEP – VI faibles
= WEP + auth. Radius
= WEP + TKIP + 802.1x + MIC
= WPA + AES + preauth.

Conclusion

- A la maison:
  - Utiliser le WEP (mieux que rien)
  - Utiliser WPA avec mot de passe partagé si disponible
- Au bureau
  - Utiliser WPA avec un serveur d'authentification Radius si disponible, sinon
  - Considérer le WLAN comme un réseau externe
    - utiliser un logiciel de type VPN dans le WLAN
    - protéger le réseau interne par un firewall

Questions


Wi Fi
CERTIFIED
Wi Fi
CERTIFIED
Interoperable with:
2.4 GHz Band
11 Mbps
54 Mbps
5 GHz Band
54 Mbps
Wi-Fi Protected Access™
www.wi-fi.org