Attaques sur RC4 et WEP

Plan

- Rappels sur RC4
  - KSA et PRGA
  - Faiblesses de RC4
- Application au WEP
  - RC4 dans le WEP
  - Diverses attaques sur le WEP
- Attaquer le WEP
  - Vue d'ensemble
  - Conséquences

Rappels sur RC4 – 1

- KSA et PRGA
  - Key Scheduling Algorithm
    - Initialisation du registre
    - A partir de la clé secrète

```
l = taille de la clé K
S = {0, 1, ..., N-1}
j = 0

Pour i de 0 à N-1:
  j = j + S[i] + K[i mod l]
  S[i] <-> S[j]
```

Rappels sur RC4 – 2

- Pseudo Random Generation Algorithm
  - Certains états sont impossibles
    - i = a, j = i+1, S[a+1] = 1
    - $1/N^2$ état dans ce cas
  - Simulation d'états trop complexe
    - Méthode « Branch and Bound »
    - Pire que la recherche exhaustive

```
i = 0, j = 0

i = i + 1
j = j + S[i]
S[i] <-> S[j]
t = S[i] + S[j]
Résultat z = S[t]
```

Rappels sur RC4 – 3

- Faiblesses de RC4
  - Faiblesse statistique du PRGA
    - Biais du PRGA : peu d'impacts
  - KSA: trop simple
    - 1 seule passe de i
    - Valeurs d'initialisation connues
    - Premiers octets de sortie reliés à la clé
  - Anomalies sur certaines clés
    - Si K[0] + K[1] = 0
    - Déduction possible de 2 octets
    - Probabilité de $2^{-10,85}$

Application au WEP

- RC4 dans le WEP
  - Sécurité du WEP débat continu
  - Clé RC4 utilisée
    - Clé de 40 bits
    - IV de 24 bits pour chaque paquet envoyé
- Diverses attaques sur le WEP
  - Recherche exhaustive de clé <1 jour
  - Construction d'un dictionnaire d'IV
  - Changement de clé trop rare
  - Dérivation de clé longue rapide

Attaquer le WEP – 1

- Vue d'ensemble
  - Conditions
    - Premier mot + IV en clair
    - Nombreux flux RC4
  - Premier mot ≈ CSTE
  - IV transmis en clair
- Les conséquences
  - Un protocole devenu obsolète
  - Beaucoup d'outils à portée de tous (LiveCD)
  - EADS cherche un PFE pour pousser plus loin

Questions

Questions ?