Kapcsolódás

Mobil eszközök kapcsolódási lehetőségei

Menyhárt László

Bevezetés

- Egymáshoz - hálózathoz
- Hogyan?
  - GSM
  - Infra
  - Bluetooth
  - GPS
  - WiFi

GSM

- Hálózat (Lefedettség)
- Automatikus (vagy nem)
- SIM kártya azonosítja az eszközt
  - subscriber identity module
  - Chip, írható rá program
  - Mikro SIM
- PIN kód azonosítja a felhasználót
  - PIN (3 rossz), PUK (Personal Identification Number, Personal Unblocking Key)

Infra

- Pont-pont kapcsolat
- Engedélyezni kell az eszköz kapcsolatot (egyet)

Bluetooth

- Kis hatótáv
- Eszköz azonosítása
- PIN kód

GPS

- Műhold folyamatosan kiabál
- GPS vevő hallgatja, számol
- Nincs azonosítás

WiFi

- Hálózat
  - WiFi hotspot (Android eszközök)
- Nagyobb távolság lehet
- SSID (Service set identifier)

WiFi - biztonság

- SSID broadcasting letiltása
- MAC address szűrés
- Jelszavak
  - WEP
  - WPA
  - WPA2

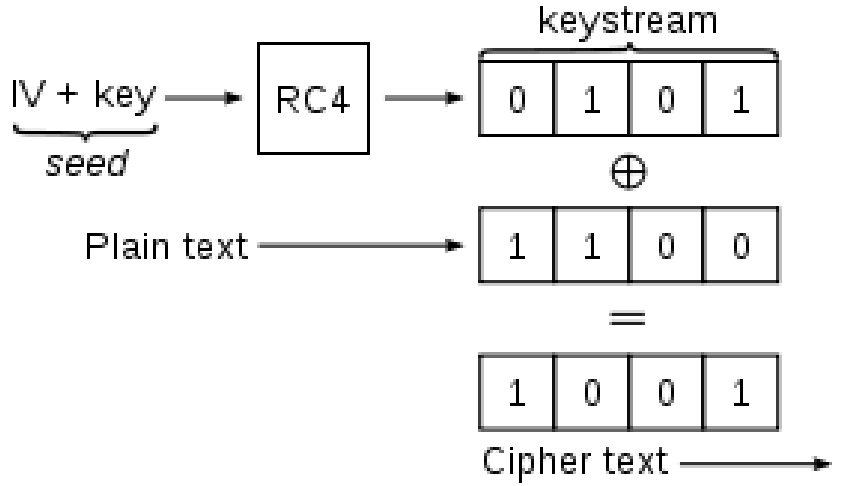
WiFi - biztonság

- WEP – Wired Equvivalent Privacy
  - 64 vagy 128-bites kódolás (RC4)
  - Ma könnyen törhető
- WPA – Wifi Protected Access
  - WPA Personal (Preshared key)
  - WPA Enterprise (Radius szerverrel)
  - WPA2 Personal (Preshared key)
  - WPA2 Enterprise (Radius szerverrel)

(Remote Authentication Dial In User Service)

WEP

- Integritás 32 bites CRC
- Titkosítás RC4 (stream)
  - Standard 64 bites:
    - 40 bites kulcs + 24 bit IV
  - 128 bites
    - 104 bites kulcs + 24 bit IV
    - 26 byte hexa kulcs
  - 256 bites
    - 232 kulcs + 24 bit IV
    - 58 byte

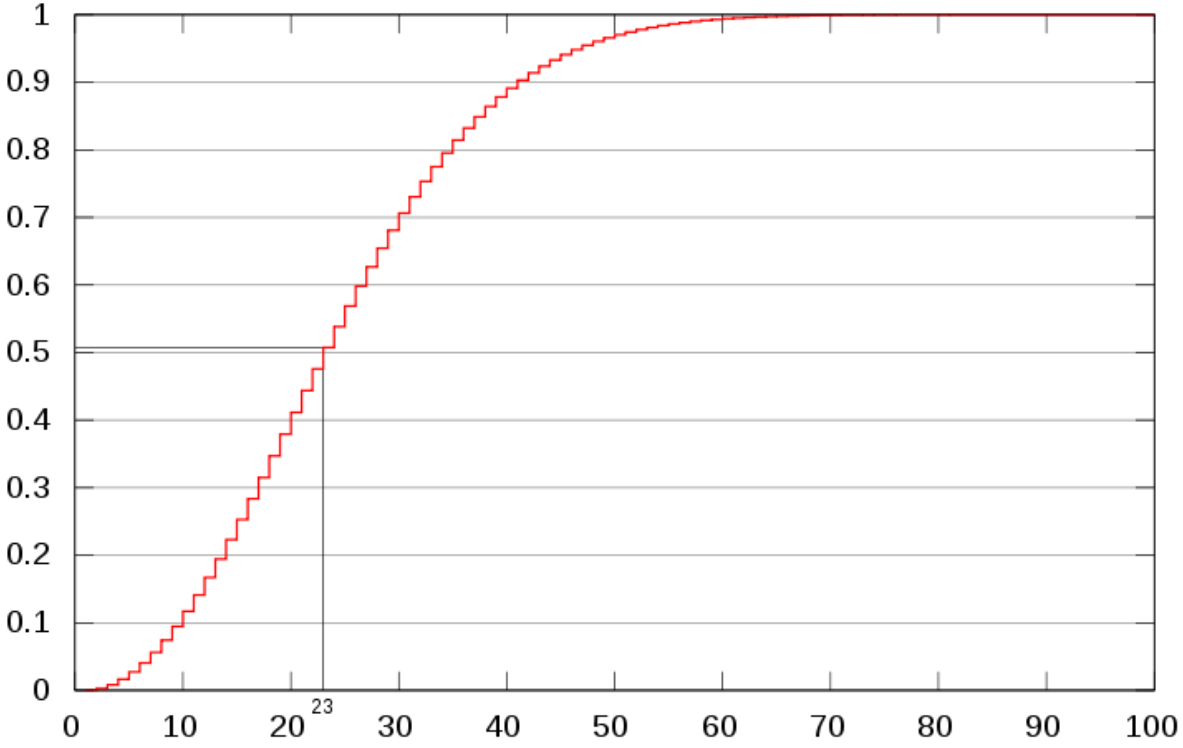


WEP azonosítás

- Open System – nincs azonosítás
- Shared Key
  - Challage-Response protokoll
    - AP véletlen szám
    - Kliens titkosítja és visszaküldi
    - Az AP kinyitja és összehasonlítás
  - A kulcs az RC4-hez is használt

WEP probléma

- Mindenki ugyanazt a kulcsot használja
- Az IV (sózás) miatt más és más a kulcs stream
- Születésnap paradoxon



Eszközök

- Ultimate tool – Backtrack CD/DVD (http://www.backtrack-linux.org/)
  - Kismet
  - Aircrack-ng
  - …

WPA

- Wifi-Protected Access
  - Ne kelljen nagyon hardware-t változtatni
  - TKIP – Temporary Key Integrity Protokoll
    - Továbbra is RC4
    - Új integritás ellenőrző algoritmus
    - IV és kulcs nem egymás után, hanem keverve
    - Az egyes adatcsomagok más kulccsal küldve
    - Támadható – 10-12 csomag injektálása a hálózatra
      → ARP poisoning

WPA2

- TKIP és AES választható
  - AES-sel nincs ismert (nyilvánosan) expolit
  - 256 bites kulcs (64 hexa digit vagy 8-63 karakter)
  - Szótáras támadás még mindig játszik
  - Jelszó → kulcs használja az SSID-t is ➔ ne legyen gyakori SSID (pl.gyártó default)
- Enterprise - EAP (Extensible Authentication Protocol)