securiteam

Vezeték nélküli hálózatok biztonsága

2015.03.29

securiTeam

Tartalom

- Miért fontos?
- Alapismeretek
- Védelmi típusok
  - WEP -Demo
  - WPA -Demo
  - WPA2
  - WPS

securiteam

Miért fontos?

- Személyes adatok védelme (bankkártya adatok)
- Nem akarod, hogy tőled lopják a netet

securiTeam

Alapismeretek

- SSID (Service Set Identifier)
  - A hálózat neve, amit látunk
- BSSID (Basic Service Set Identifier)
  - A csatlakozás pont (AP) MAC címe

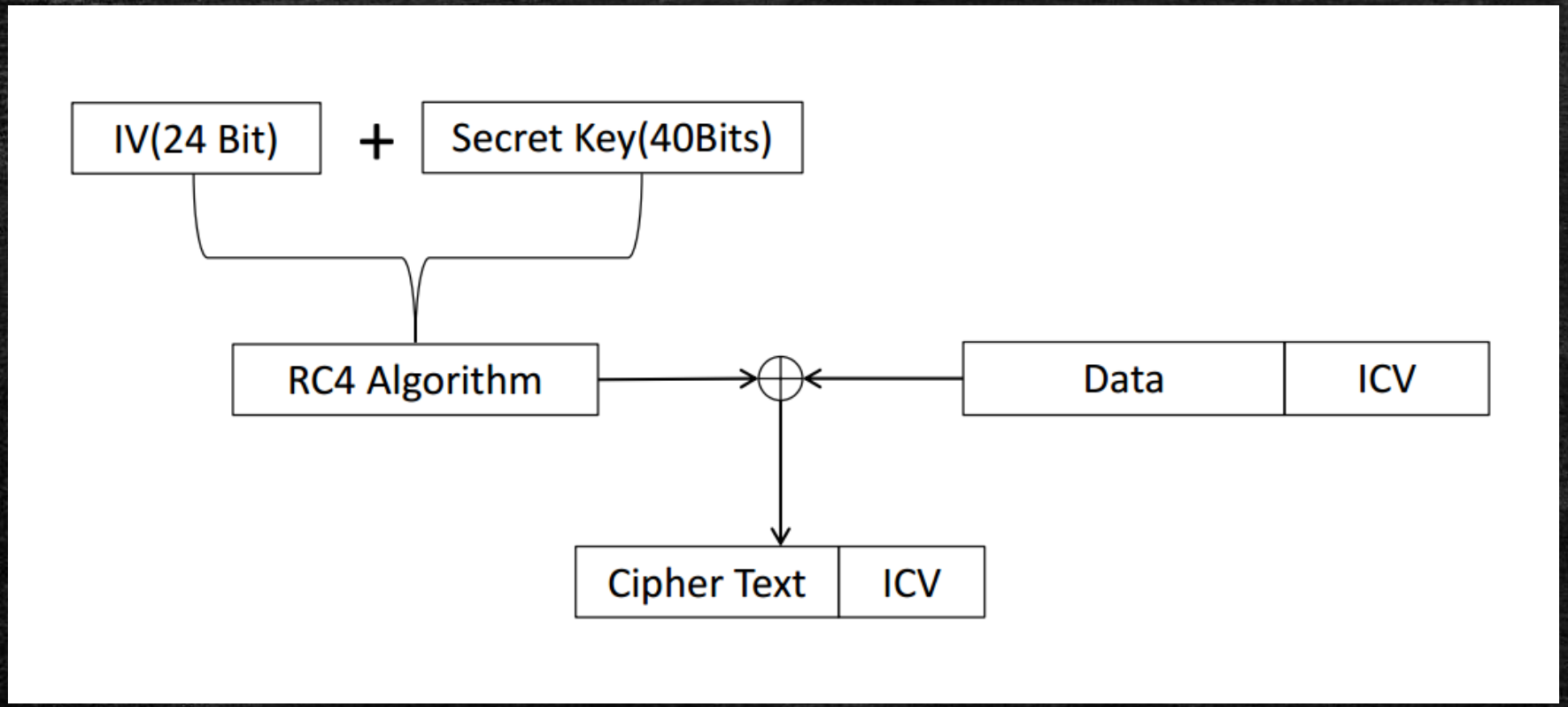
securiTeam

WEP (Wired Equivalent Privacy)

- IEEE 802.11 része
- Csatornatitkosítás alapú
- Rosszul kivitelezett algoritmus (RC4)
- WEP-40 és WEP-104 (+24 IV -> 64 & 128)
- Két autentikációs típusa van
  - Open System Authentication
  - Shared Key Authentication

securiTeam

WEP titkosítás



securiTeam

Demo

securiTeam

WPA (Wi-Fi Protected Access)

- Firmware update
- WEP legnagyobb hiányosságait javította
- PSK autentikáció -> törhető szótárral (brute forccal nagyon sokáig tart)
- TKIP kódolás -> sebezhető

securiTeam

WPA2

- PSK autentikáció -> törhető szótárral
- AES (CCMP) titkosítás (máig töretlen!)
- Nyerő kombináció WPA2-AES erős jelszóval (legalább 12 karakter, nagybetű, kisbetű, szám, speciális karakter)

securiTeam

Demo

WPS (Wi-Fi Protected Setup)

- Push Button Connect
- PIN
  - External
  - Internal

securiTeam

WPS External PIN

- Rossz kivitelezés
- 10^3+10^4 kombináció
- Az újabb routerek már tudnak védekezni ellenne pl.: timeoutolással

securiTeam

Köszönom a figyelmet!

- Források
  - Wikipedia
  - Kali Tutorials
  - Blackmoreops