WEP verschlüsseltes WLan

Auf mit der veralteten Verschlüsselungstechnik WEP für drahtlose Netzwerke existieren einige gut funktionierende Angriffe. Voraussetzung für einen schnellen Erfolg ist jedoch ausreichender Datenverkehr im angegriffenen Netzwerk - wenn ein WEP-gesichertes Netz keine Teilnehmer hat, ist die Wahrscheinlichkeit gering, den Schlüssel schnell zu berechnen, da man nicht genügend Datenpakete mitschneiden kann. Die meisten Angriffe nutzen die Schwachstelle des mit 24 Bit sehr kurzen Initialisierungsvektor IV bei der RC4-Verschlüsselung aus. Diese Angriffsmethode wird häufig als Related-Key-Attack bezeichnet.