

Šifrování v bezdrátových sítích

Sítě zabezpečené protokolem WEP používají pro utajení obsahu komunikace šifru RC4. Jedná se o proudovou šifru, která v každém kroku vygeneruje pseudonáhodný byte na základě svého vnitřního stavu. Šifrování i dešifrování spočívá v kombinaci vygenerovaného proudu bytů a utajované zprávy pomocí bitové operace XOR. Vnitřní stav je pole (S) o 256 položkách určujících permutaci všech možných hodnot bytu a dva indexy (i , j) do tohoto pole. Generovaný byte je určen jako $S[S[i] + S[j]]$, v každém kroku jsou prohozeny prvky na pozicích i , j a indexy jsou aktualizovány. Stav je inicializován klíčem délky nejvýše 256 bytů, obvykle však nepřekračujícím 16 bytů.

RC4 neurčuje, jakým způsobem použít dlouhodobý klíč pro ustanovení vlastního šifrovacího klíče (u proudových šifer není bezpečné použít stejný iniciální stav pro různá data). V případě WEP je klíč vytvořen zřetěžením 40-bitového, resp. 104-bitového klíče a 24-bitového v čase proměnného inicializačního vektoru. Kvůli nízké bitové délce vektoru se ale klíče časem začnou opakovat a při odchycení dostatečného provozu v síti může být šifra snadno prolomena. Díky kombinaci pouhým zřetěžením se také otvírá cesta k útokům přes podobné klíče (related key attacks), vůči kterým je RC4 zranitelná. V případě krátkého klíče může být algoritmus také prolomen jednoduchým útokem hrubou silou (vyzkoušením všech možných klíčů).

Původní protokol WPA spoléhá také na šifru RC4 (kvůli zpětné kompatibilitě s hardwarem), používá ale protokol TKIP pro ustanovení dočasných klíčů. Dlouhodobý klíč a inicializační vektory jsou v něm lépe kombinovány a každý paket je zašifrován odlišným nepodobným klíčem, takže nehrozí útoky zneužívající slabiny RC4 jako u WEP. Novější verze WPA – WPA2 – používá pro utajení protokol CCMP. Ten nahrazuje RC4 standardizovanou blokovou šifrou AES se 128-bitovým klíčem, u níž nejsou známy žádné zásadní bezpečnostní zranitelnosti, a podstatně zvyšuje bezpečnost bezdrátové komunikace.