



Podstawowe fakty dotyczące sieci IPv4

- ▶ Warstwa sieciowa IP nie gwarantuje żadnej poufności danych (ani szyfrowania). W IPv4 wszystkie dane przesyłane są „otwartym tekstem”. Szyfrowanie i kontrola integralności danych muszą być implementowane w wyższych warstwach, jeśli są konieczne.
- ▶ Dane przesyłane siecią komputerową mogą zostać podsłuchane. Skoro przesyłamy dane otwartym tekstem, a pakiety przechodzą przez wiele routerów i sieci, to we wszystkich tych miejscach może znajdować się ktoś, kto podsłuchuje nasze pakiety.
- ▶ Często musimy zaufać danym uzyskiwanym z serwerów znajdujących się poza naszą kontrolą. Wiele informacji o kluczowym znaczeniu (np. nazwy hostów zwracane przez DNS) jest zwracane przez serwery znajdujące się poza kontrolą lokalnego administratora, a więc niekoniecznie godnych zaufania.
- ▶ IPv4 i protokoły sieciowe projektowano z reguły nie biorąc pod uwagę zagrożeń bezpieczeństwa. Pakiety IP mogą być fałszowane, przechwytywane, modyfikowane i przekierowywane, podsłuchiwanie. Można się też z ich pomocą podszywać pod inne urządzenia sieciowe lub hosty.
- ▶ Wiele protokołów projektowanych z myślą o poprawieniu bezpieczeństwa jest tak naprawdę tylko obejściem problemu, a nie jego prawdziwym rozwiązaniem, które często jest niemożliwe.
- ▶ Największa zaleta sieci IP – nieograniczona enkapsulacja warstw oprogramowania i elastyczność stosowania poszczególnych rozwiązań – są także najsłabszymi elementami, jeśli chodzi o bezpieczeństwo.
- ▶ Rozszerzenia protokołów związane z bezpieczeństwem muszą być wprowadzane jako osobne warstwy protokołów i dopiero po powszechnej akceptacji (do tego czasu – eksperymentalnie, tak jak np. SSL, IPSec)