

# Autentizace

Autentizace je proces ověření (a tím i ustavení) identity subjektu (s požadovanou mírou záruky). Je to proces, kdy se posuzuje, zda je subjekt žádající přístup k síti oprávněným uživatelem sítě. Na základě úspěšné autentizace je subjektu povolen přístup do sítě.

Používají se tyto základní metody pro zjištění identity:

- Podle toho, co uživatel zná (např. heslo, PIN)
- Podle toho, co uživatel má (např. hardwarový klíč, čipová karta, ...)
- Podle toho, čím uživatel je (biometrické vlastnosti uživatele - např. otisk prstu, snímek oční duhovky, ...)
- (případně kombinace přecchozích)

## ***V bezdrátových sítích jsou známe následující metody autentizace:***

### Open system

Subjektu je přístup do sítě povolen na základě žádosti bez jakéhokoliv ověření. Takový systém neposkytuje žádnou úroveň zabezpečení. Je vhodný pro veřejné bezdrátové sítě, kde není vyžadováno žádné zabezpečení.

### Filtr MAC adres

Přístup do sítě je povolen pouze předem schváleným MAC adresám. Přenášené MAC adresy se nijak nešifrují, případný útočník je proto může odposlechnout a poté se vydávat za zařízení s takovou adresou. Tato metoda zabrání přístupu do sítě pouze náhodným útočníkům, kteří nemají dostatečné znalosti.

### Autentizace na základě znalosti identifikátoru Wi-Fi sítě

Technika skrývání identifikátoru SSID - identifikátor je sdělen pouze stanicím, které mají povolený přístup do sítě. Stanice se dostanou do sítě pouze tehdy, když prokáží znalost tohoto identifikátoru. Zasílaný identifikátor není šifrován, znalý útočník ho může odchytit a následně použít pro přístup do sítě. Tato metoda nepřináší vyšší zabezpečení bezdrátové sítě.

### WEP

Autentizace na základě protokolu WEP - šifrování pomocí statických WEP klíčů symetrické šifry, v současnosti zabrání přístupu do sítě pouze náhodným útočníkům. Kvůli nedostatkům v protokolu lze zachycením specifických rámců a jejich analýzou velmi snadno získat klíč používané šifry.

### WPA/WPA2

Zabezpečení WPA je reakce na prolomení zabezpečení pomocí WEP. Autentizace do WPA sítě je prováděna buď pomocí PSK(Pre-Shared Key, autentizace na základě hesla) nebo pomocí RADIUS server (ověřování přihlašovacím jménem a heslem).

### RADIUS

Autentizace na základě služby RADIUS probíhá pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Uživatelská jména jsou přes síť vždy zasílána šifrovaně.