Zabezpečení WiFi sítí

zpracoval Zdeněk Styblík
pod vedením Ing. Alexandra Vasilenka

> cíl práce

- porovnání mechanismů zabezpečení používaných ve WiFi sítích
- poukázat na jejich případné nedostatky
- pokusit se prakticky tyto nedostatky ověřit
- ukázat, že nastavení silného zabezpečení je poměrně jednoduché (? :)

> metodika

- použití operačního systému GNU/Linux
- aplikace aircrack-ng na prolomení zabezpečení
- aplikací ettercap, Kismet, tcpdump
- a dalších...

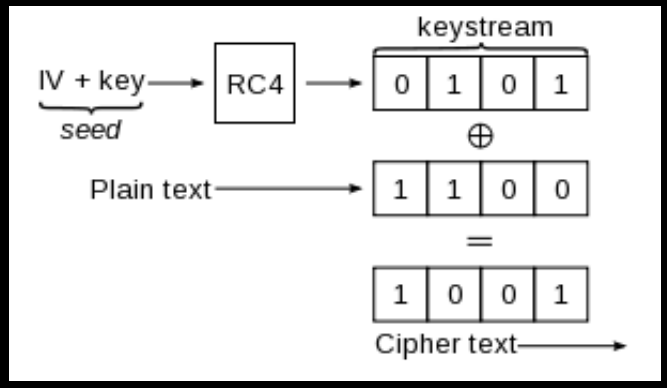
- všechna testování byla provedena na testovací sítí k tomu určené (přísahám! :)

> layer 2/3

- zabezpečení na linkové/síťové vrstvě
- data nejsou šifrována
- ochrana pouze před „Běžným Františkem Uživatelem“
- velmi lehké na prolomení (řádově minuty)
- vhodné spíše jako doplňek k ostatním mechanismům

> wep

- základní zabezpečení (šifrováním)
- náročnější na prolomení (řádově desítky minut)
- slabinou je časté opakování klíče
- nástupcem je WPA/WPA2 a to od r. 2004
- stále nejpoužívanější způsob „zabezpečení“



> wpa

- náhrada za WEP
- dnes již podpora na všech zařízeních
- velmi náročné na prolomení (hw + čas)
- v r. 2008 objevena slabina v TKIP
- „slabé“ předsdílené heslo (pre-shared key) může ulehčit průlom

> wpa2

- náhrada za WPA
- prolomení může trvat hodiny, dny, měsíce
- implementuje prvky ze standardu IEEE 802.11i
- implementuje AES algoritmus a CCMP protokol
- WPA2 Personal = AES/TKIP+AES
- WPA2 Enterprise = implementace 802.1x

> 802.1x

- nevhodné pro domací využití
- vhodné pro podnikové sítě a WAN/MAN sítě
- nutná vysoká dostupnost authentikačního serveru
- nastavení serveru vyžaduje know-how
- vhodné v kombinaci s IPsec

> závěr

- žádné zabezpečení není 100% spolehlivé
- nastavení zvládne i běžný uživatel
- mechanismy je vhodné kombinovat
- volit vhodné klíče = kombinace písmen, číslic a znaků resp. stejná politika jako pro hesla

> prostor pro vaše dotazy

@ konec