Zaštita bežičnih mreža

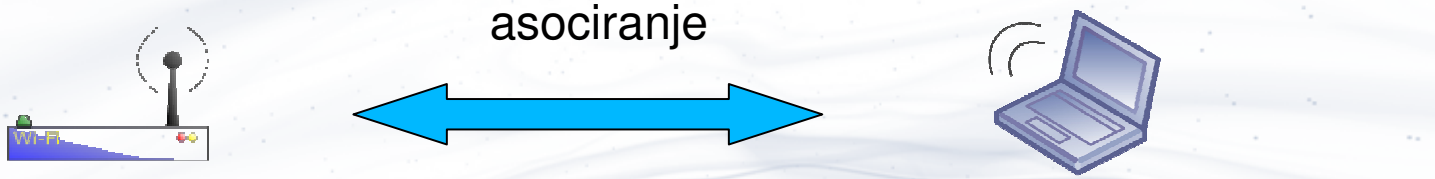
Krešimir Nesek
CARNet CERT

Sadržaj

- Uvod
- Sigurnosni mehanizmi
- Prijetnje
- Kako se zaštititi

Uvod – 802.11

- IEEE 802.11 bežične mreže



AP – access point
pristupna točka

STA – wireless station
bežična stanica

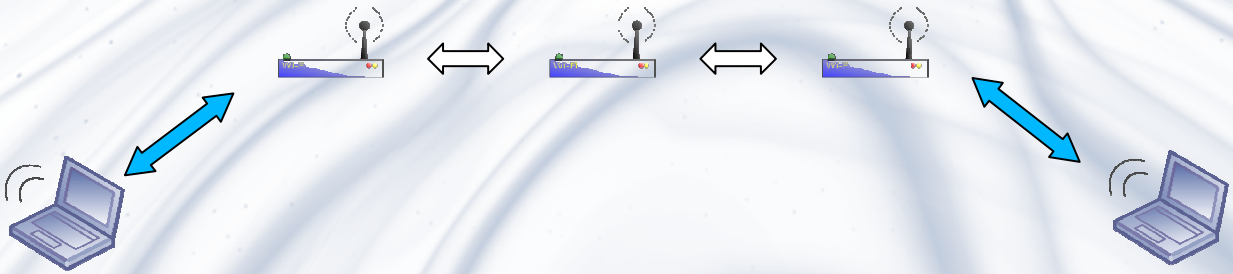
- SSID – service set id - naziv mreže

Uvod - konfiguracije

- Infrastructure

- Ad – hoc

- WDS



Stupnjevi sigurnosti

- Otvoreni sustav
  - bilo koji klijent se može asocirati
    - moguće je filtrirati MAC adrese
    - skrivanje SSID-a
  - podaci nisu kriptirani
- WEP
  - za spajanje je potrebno poznavati ključ
  - podaci su kriptirani
- WPA i WPA2
  - za spajanje je potrebno:
    - poznavati lozinku ili koristiti 802.1x autentikaciju
  - podaci su kriptirani

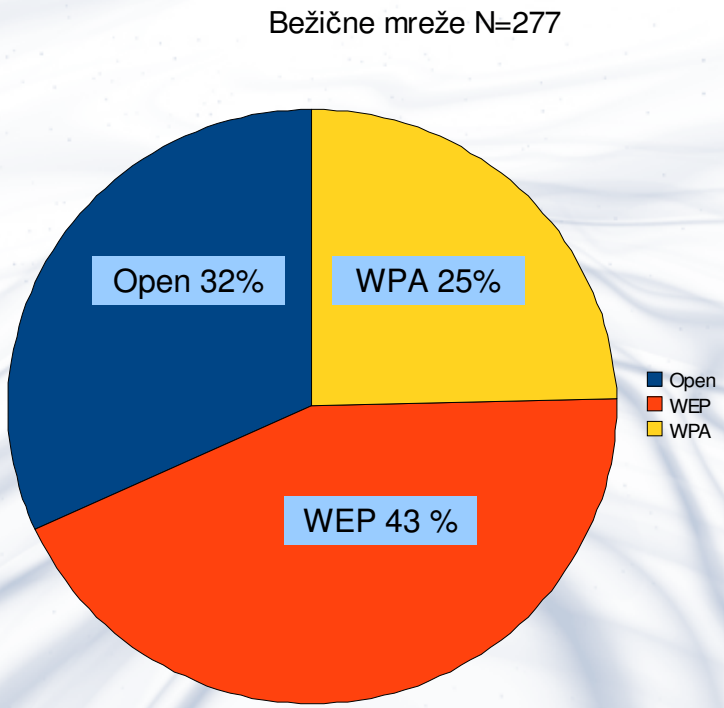
CERT.hr

Stanje u svijetu

- World-wide war-drive istraživanje
  - ljudi iz raznih dijelova svijeta dostavljaju informacije o bežičnim mrežama u svojoj okolici
- 2003. godina
  - 67% nema zaštite (uzorak: 88122)
- 2004. godina
  - 62% nema zaštite (uzorak: 228537)

Stanje u Hrvatskoj

- Zagreb, 2007.
- 32% mreža je otvoreno



Sigurnosne prijetnje - otvoreni sustav

- Bilo koji klijent se može asocirati
  - pa i potencijalni maliciozni korisnici
- Promet nije kriptiran
  - bilo tko može prisluškivati komunikaciju
  - man-in-the-middle napadi
- Sakrivanje SSID-a
  - lako se otkriva prisluškivanjem
- Filtriranje MAC adresa
  - prisluškivanjem se lako saznaju autorizirane MAC adrese
  - MAC adresa se jednostavno krivotvori

WEP

- Wired Equivalent Privacy
  - cilj je riješiti problem privatnosti podataka u bežičnoj mreži
- podaci se kriptiraju
- RC4 enkripcijski algoritam
- 64 ili 128 bitni ključ
- za asociranje klijenti moraju znati ključ

WEP – probijena zaštita

- nedostaci u dizajnu
- WEP zaštita je probijena
  - postoje javno dostupni alati za probijanje WEP-a
  - WEP ključ – za manje od 5 minuta
- cilj nije ostvaren

Otvoreni sustav i WEP – mjere opreza

- Uključiti vatrozid na računalu
  - provjeriti pravila vatrozida, lokalna mreža nije sigurna
- Sav nekriptirani promet nije siguran
  - pažljivo provjeravati certifikate
- VPN

WPA i WPA2

- WiFi Protected Access
- Ispravlja nedostatke WEP-a
- Koristi ključeve koji se mijenaju za vrijeme korištenja sustava
- WPA2 koristi AES umjesto RC4

WPA i WPA2 – kontrola pristupa

- Pre-shared key mode
  - za spajanje je potrebno znati unaprijed određeni ključ – lozinku
- Enterprise mode
  - za autentikaciju se koristi 802.1x protokol
  - potreban je autentikacijski poslužitelj
  - moguća je autentikacija na razini korisnika (username – password)

WPA i WPA2 – sigurnosne mjere

- napadi na WPA osiguranu mrežu svode se na *brute force* napade pogađanjem lozinke
- važno je postaviti dobru lozinku
  - ne koristiti riječi iz rječnika
  - čim veća duljina lozinke
  - koristiti mala i velika slova, brojke i specijalne znakove

Zaključak

- koristiti WPA ili WPA2
  - 802.1x autentikacija
  - jaka lozinka
- oprez prilikom spajanja na otvorenu mrežu

Pitanja

Hvala na pažnji ☺

Krešimir Nesek

Kresimir.Nesek@CARNet.hr