

CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

Sigurna bežična mreža u Linux okruženju

Antonia Kujundžić

Sadržaj:

- Potrebe korisnika vs. (ne)sigurna bežična mreža
- Moguća rješenja
- Implementacija u Linux okruženju

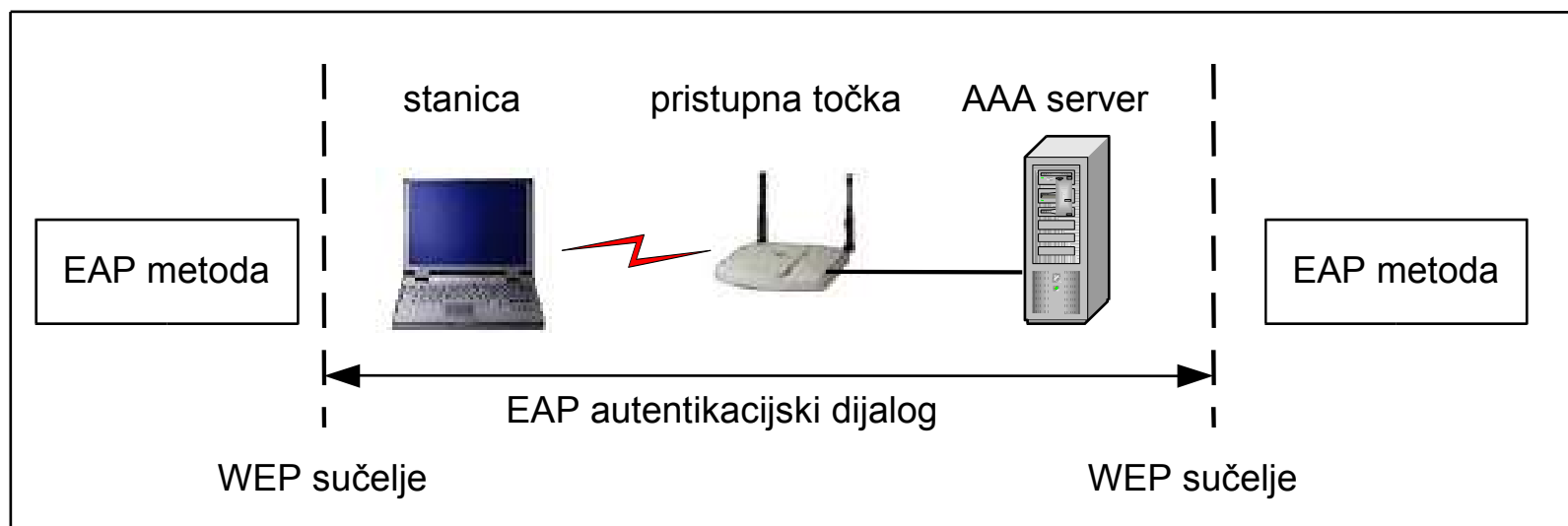
Potrebe korisnika vs. (ne) sigurna bežična mreža

- ▣ jedinstvena identifikacija korisnika
- ▣ korištenje postojeće autentikacijsko-autorizacijske infrastrukture (RADIUS - LDAP)
- ▣ pristup “gostujućih” korisnika
- ▣ Linux desktop

Moguća rješenja

- Statički WEP (nesiguran)
- autentikacija po MAC adresi (nesigurna)
- pojedine EAP metode koje podržava standard IEEE 802.1x, npr. LEAP, PEAP (*proprietary*)
- WEB gateway (*“hard to make safe”*)
- VPN pristup (*“hard to make scalable”*)
- EAP metode: TLS (certifikati na strani klijenta i poslužitelja), **TTLS** (korisničko ime, lozinka, prihvaćanje poslužiteljskog certifikata na strani klijenta, dinamički WEP ključevi)

Implementacija



Implementacija na strani stanice (1)

- ▣ Open1x – Xsupplicant (free)
 - nestabilan (trenutna verzija 0.8b)
 - upitna implementacija dinamičkog WEP-a
 - loše korisničko sučelje
 - ne podržava sve EAP metode (npr. EAP-SIM)

Implementacija na strani stanice (2)

- ▶ Meetinghouse AEGIS Client (not so free :)
 - ▶ nije inicijalno namijenjen za Debian , već za RH distribuciju - rađene su manje izmjene
 - ▶ stabilan
 - ▶ jednostavno grafičko sučelje
 - ▶ podržava sve poznatije EAP metode

Implementacija na strani pristupne točke

- podrška za standard IEEE 802.1x
- testirani uređaji: Compaq WL510 (nema podršku za protokol EAP, nema načina nadogradnje)
- Cisco Aironet 350, 1100, 1200 (sadrži svu potrebnu podršku, IOS se konstatno nadograđuje)
- način implementacije: definicija SSID-a (VLAN), definicija RADIUS poslužitelja, definicija statičkog WEP ključa.

Implementacija na strani AAA poslužitelja

- ▶ FreeRADIUS (free)
 - ▶ open source
 - ▶ relativno stabilan
 - ▶ konfigurabilan
 - ▶ podržava sve EAP metode
- ▶ Lucent Navis Radius (not so free :)
 - ▶ prilično komplicirana konfiguracija – grafičko sučelje u kombinaciji sa java editorom
 - ▶ loša realizacija za neke EAP metode (TLS)
 - ▶ vrline: može određene zahtjeve prosljeđivati definiranom LDAP-u, te istovremeno za druge zahtjeve biti proxy - FreeRADIUS nažalost to ne može

Zaključak

- iako open source alati za bežičnu mrežu općenito još uvijek sasvim ne zadovoljavaju potrebe sigurne bežične mreže – imaju velik potencijal!



Antonia.Kujundzic@CARNet.hr