Radijske pristupne mreže

Leonard Novosel, mag. ing.

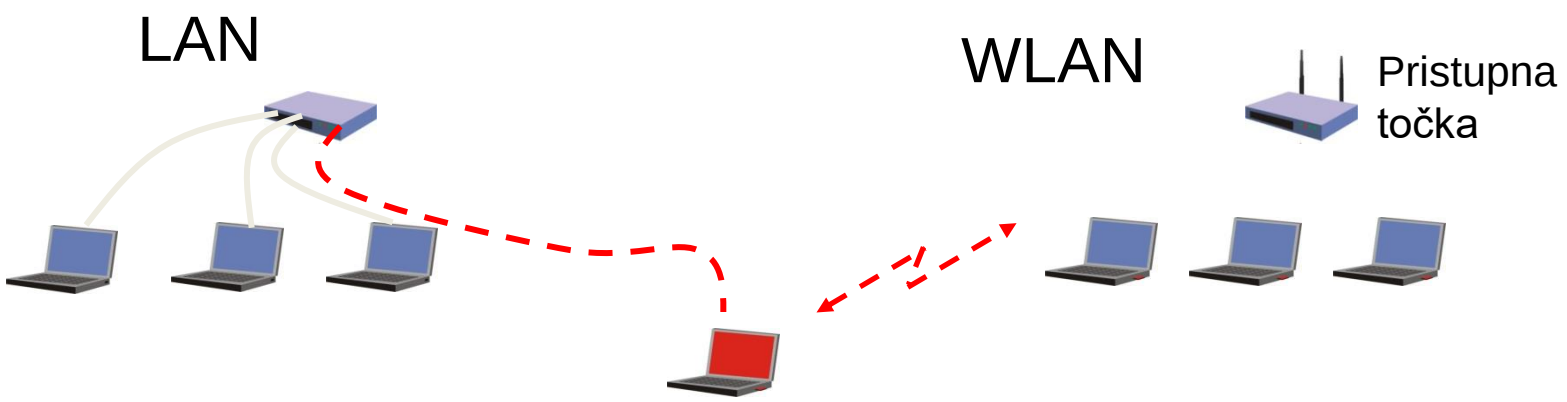
Sigurnost u WLAN-u

Sadržaj

- Uvod
- Kriptografija
- Osnovni sigurnosni standardi u radijskim mrežama
  - WEP
  - WPA(2)
- Zaštita WLAN mreža
  - MAC filtriranje
  - SSID skrivanje
- Napad na WLAN mreže

Uvod

- IEEE 802.11 je skupina IEEE normi koja definira radijske (bežične) računalne mreže
- prednosti WLAN mreža u odnosu na LAN mreže su:
  - jednostavnost spajanja na mrežu
  - mobilnost
- glavni nedostaci WLAN mreža u odnosu na LAN mreže su:
  - manja brzina prijenosa podataka
  - **SIGURNOST !!!**



Kriptografija

- *"Cryptography is the art of keeping messages secure"*, Bruce Schneier
- Pojmovi:
  - kriptografija: znanstvena disciplina koja se bavi skrivanjem podataka ili njihovom izmjenom u neki neprepoznatljiv oblik
  - običnitekst: originalna poruka
  - šifrirani tekst: poruka nakon šifriranja
  - šifriranje: kodiranje originalne poruke u svrhu skrivanja njenog značenja
  - dešifriranje: vraćanje originalne poruke iz šifrirane

Kriptografija (nastavak)

- većina današnjih sustava za prijenos podataka oslanja se na neki oblik šifriranja podataka u svrhu njihove zaštite
- zaštite WLAN mreža uglavnom koriste ključeve i certifikate pomoću kojih se šifriraju podaci i o(ne)mogućava pristup pojedinoj mreži
- samo šifriranje izvedeno je primjenom operacije isključivo ILI (XOR) nad podacima koje želimo sakriti
- drugi operand koji se koristi u toj operaciji je ključ ili se operand stvara od ključa i dodatnih podataka

Osnovni sigurnosni standardi u radijskim mrežama

- osnovni sigurnosni algoritmi koji se koriste u zaštiti radijskih mreža su:
  - **WEP** (*Wired Equivalent Privacy*)
  - **WPA** (*Wi-Fi Protected Access*)
  - **WPA2/RSN** (*Robust Secure Network*)
- iako većina moderne mrežne opreme podržava sve od navedenih sigurnosnih protokola, razina sigurnosti koju oni pružaju se uvelike razlikuje
- WEP algoritam u odnosu na WPA/WPA2 pruža mnogo manju razinu sigurnosti – probijanje WEP zaštite ne predstavlja veliki problem
- važno je naglasiti da nijedan algoritam za zaštitu ne može štititi mrežu od radijskog ometanja koje izaziva uskraćivanje usluge **DoS** (*Denial-of-Service*)

WEP (*Wired Equivalent Privacy*)

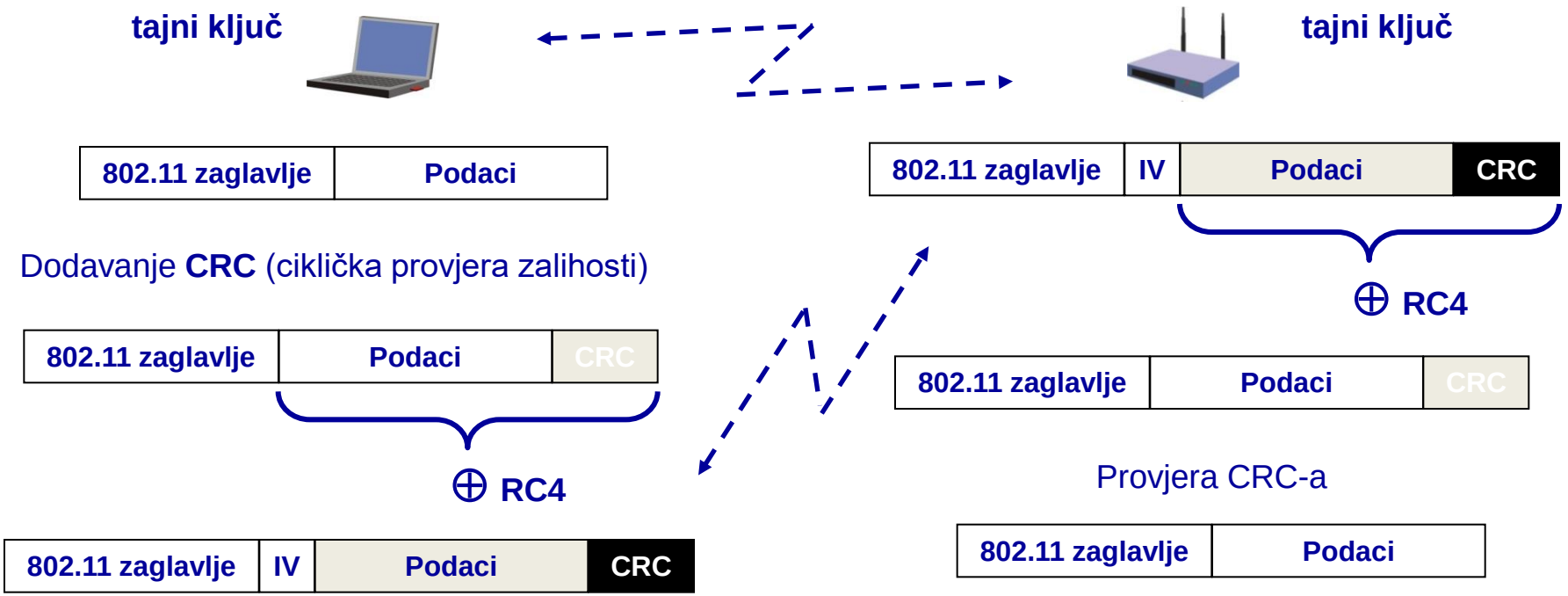
- prvi sustav zaštite 802.11 mreža
- predstavljen je 1997. godine
- cilj je bio pružiti zaštitu radijskih mreža sumjerljivu klasičnim, žičnim mrežama
- WEP nudi tri bitna zaštitna servisa:
  - tajnost/povjerljivost podataka (*Confidentiality*)
  - integritet podataka (*Integrity*) – provjera duljine primljenog okvira u svrhu detekcije promjene podataka u prijenosu
  - kontrola pristupa (*Authentication*) – omogućavanje pristupa samo korisnicima koji posjeduju odgovarajući tajni ključ

WEP (nastavak)

- WEP algoritam koristi slijednu šifru (*stream chiper*) zasnovanu na **RC4** enkripcijskom algoritmu
- RC4 (Rivest Cipher 4) osmislio je Ron Rivest 1987. iz RSA Security
- RC4 slijedna šifra dobiva se pomoću tajnog ključa i inicijalizacijskog vektora (**IV**)
- pomoću slijedne šifre šifriraju se podaci uporabom **XOR** (isključivo ILI) operatora
- na prijamnoj strani, podaci se inverznim postupkom dešifriraju
- primjenjivo je na podatke različite duljine
- nedostatak je nezaštićenost nepodatkovnih okvira, pa je moguća analiza prometa bez posjedovanja šifre

WEP (nastavak)

- Postoji nekoliko vrsta WEP standarda:
  - 64-bit WEP (40 bitni tajni ključ + 24 bitni IV)
  - 128-bit WEP (104 bitni tajni ključ + 24 bitni IV)
  - WEP2, 256 bita (232 bitni tajni ključ + 24 bitni IV)



WEP (nastavak)

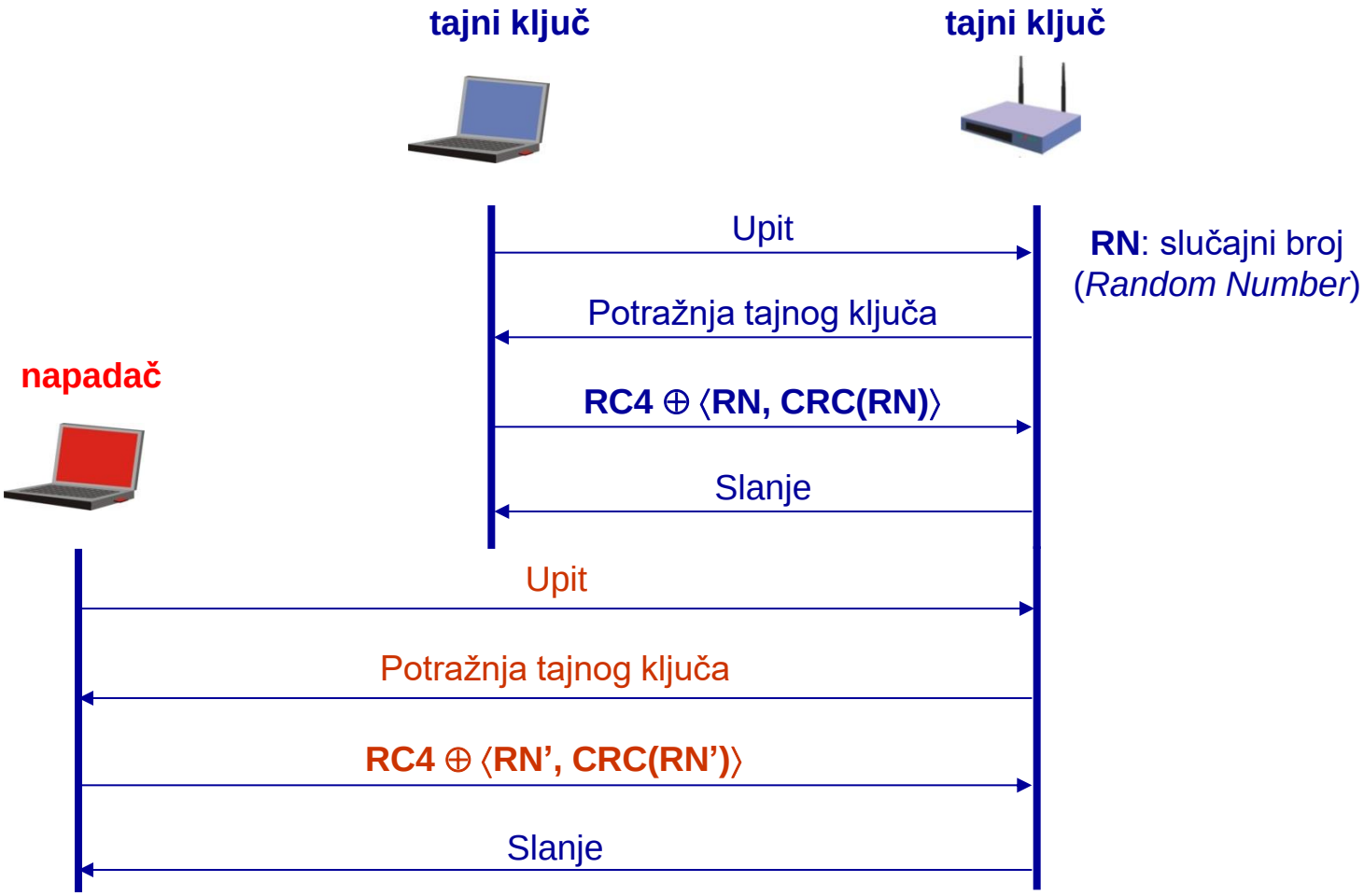
- Glavni nedostaci WEP standarda:
  - isti IV se koristi više od jednom
  - 24 bitni IV daje 1677216 kombinacija (norma IEEE 802.11)
  - koriste se stalni, a ne privremeni tajni ključevi
  - većina korisnika ne mijenja svoje tajne ključeve
- IV se mijenja za svaki odaslani paket
- ako se IV generira na slučajan način, dva paketa će imati istu vrijednost nakon manjeg broja paketa nego da se IV generira po redu, to se naziva "*birthday paradox*"
- ako se IV jednostavno uvećava, dva računala koja odašilju stalno će stvarati pakete sa istom vrijednošću IV-a

WEP (nastavak)

- Primjer napada na sustav zaštićen WEP algoritmom:
  - ako je 24 bitni IV implementiran kao rastući brojač
  - ako pristupna točka odašilje brzinom od 11 Mbit/s
  - svi IV će biti iskorišteni unutar otprilike **5 sati**
  - napadač prikuplja sav promet
    - napadač traži dvije poruke s istim IV
    - otkriva se tekst poruke koji je zaštićen
    - tekst poruke $\oplus$ tajni ključ = RC4
  - s obzirom na generator pseudoslučajnih brojeva, nije potrebno prikupljati sav promet

WEP (nastavak)

- Primjer napada na sustav zaštićen WEP algoritmom:



WEP (nastavak)

- WEP je unatoč ne baš kvalitetnom početnom rješenju doživio unaprjeđenja s kojima je postignuta dovoljna razina sigurnosti
  - 802.1X pruža kontrolu pristupa korisnika i upravljanje ključevima (predstavljen 2001.)
  - 802.11i bavi se tajnošću i integritetom podataka
- Upotreba RC4 zaštite zamijenjena je AES-om (*Advanced Encryption Standard*)

WPA(2) (*Wi-Fi Protected Access (II)*)

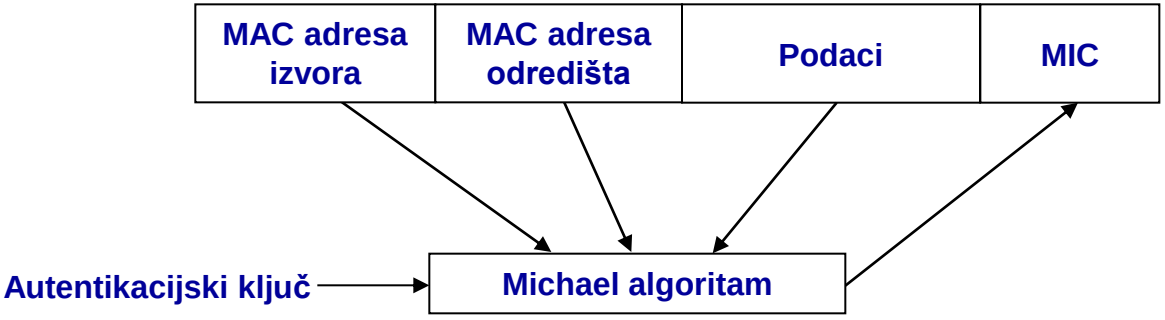
- otklanja nedostatke WEP algoritma
- omogućava korištenje postojećeg hardvera (WPA)
- WPA implementira glavninu norme 802.11i
- Pojmovi vezani uz WPA:
  - **TKIP** - *Temporal Key Integrity Protocol*
  - **MIC** - *Message Integrity Code* (zamjenjuje CRC)
  - **AES** - *Advanced Encryption Standard*
  - **PSK** - *Pre-Shared Key mode*
  - **TLS** - *Transport Layer Security*
  - **EAP** - *Extensible Authentication Protocol*
  - **LEAP** - *Light* EAP (Cisco)
- WPA2 zahtjeva promjenu postojećeg hardvera
- nova oprema mora biti kompatibilna s WPA2

WPA(2) (*Wi-Fi Protected Access (II)*) **(nastavak)**

- **TKIP** - *Temporal Key Integrity Protocol*
  - izrađen unutar 802.11i grupe
  - koristi tri nove značajke u cilju poboljšanja sigurnosti u WEP mrežama
    - povećava incijalizacijski vektor na 48 bita
    - koristi sekvencijski brojač za zaštitu od napada ponavljanjem poruke “replay”
    - koristi novi 64-bitni mehanizam za zaštitu integriteta (MIC, *Message Integrity Check*) “Michael”

WPA(2) (*Wi-Fi Protected Access (II)*) (nastavak)

- **MIC** - *Message Integrity Code* (8 okteta)
  - autentikacijski ključ dobiva se iz **PTK** (*Pairwise Transient Key*)
  - posljednjih 16 okteta PTK tvore autentikacijski ključ (128 bita)
    - 8 okteta služi za izračun MIC-a za pakete koje šalje pristupna točka
    - 8 okteta služi za izračun MIC-a za pakete koje šalje korisnik



WPA(2) (*Wi-Fi Protected Access (II)*) **(nastavak)**

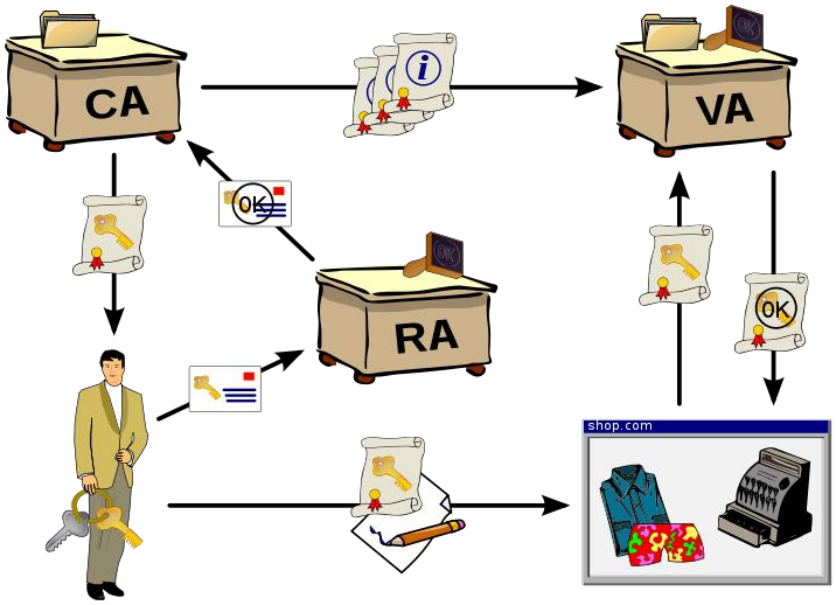
- **AES** - *Advanced Encryption Standard*
  - šifriranje pomoću simetričnog ključa
  - postao standardom 2002. (NIST - *National Institute of Standards and Technology*)
  - duljina bloka je 128 bita, a duljina ključa može biti 128, 192 ili 256 bita
  - ovisno o duljini ključa ulazna poruka se šifrira određeni broj puta zamjenom bitova i permutacijom redaka i stupaca
    - 10 puta za 128-bitni ključ
    - 12 puta za 192-bitni ključ
    - 14 puta za 256-bitni ključ
  - neobavezno korištenje u WPA, obavezno u WPA2

WPA(2) (*Wi-Fi Protected Access (II)*) **(nastavak)**

- **PSK** - *Pre-Shared Key mode*
  - dizajn za kućne i uredske mreže
  - svaka mreža koristi svoj 256 bitni ključ
  - nema potrebe za korištenjem poslužitelja za provjeru vjerodostojnosti kao kod 802.1X
  - ključ može biti niz od 64 heksadecimalne znamenke ili šifra od 8 do 63 ASCII znaka

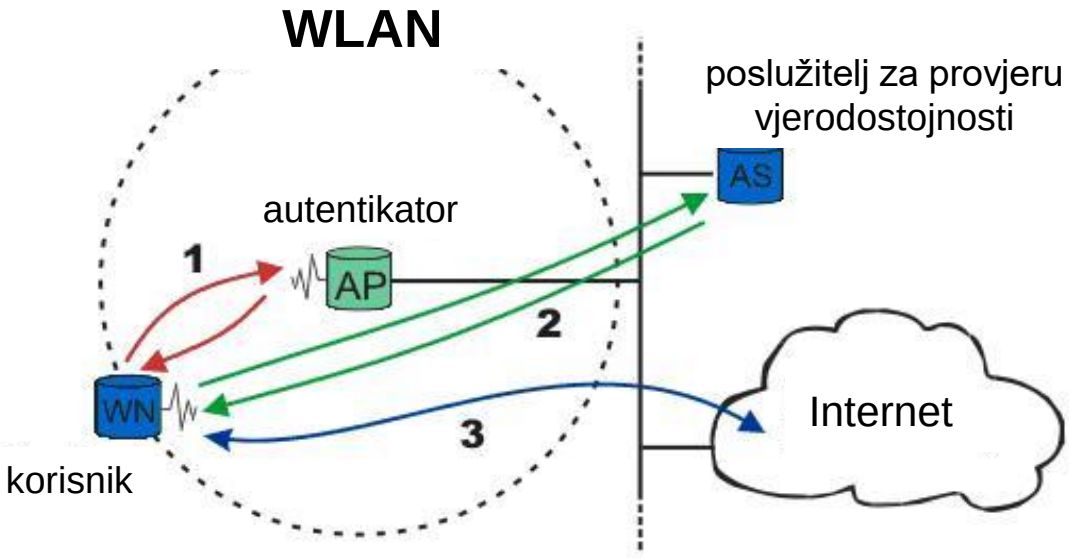
WPA(2) (*Wi-Fi Protected Access (II)*) (nastavak)

- **PKI** – *Public Key Infrastructure*
  - povezivanje javnih ključeva s korisničkim identitetima
  - **CA** – *Certificate Authority* je izdavač certifikata
  - **RA** – *Registration Authority* je verifikator certifikata
  - **VA** – *Validation Authority* se brine o ispravnosti certifikata klijenta



WPA(2) (*Wi-Fi Protected Access (II)*) (nastavak)

- **EAP** - *Extensible Authentication Protocol*
  - koristi se unutar norme 802.1X
  - koristi se poslužitelj RADIUS (*Remote Authentication Dial In User Service*) za provjeru vjerodostojnosti korisnika
  - autentikator (pristupna točka) služi kao most između korisnika i poslužitelja za provjeru vjerodostojnosti
  - postoji oko 40 vrsta EAP protokola (EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP,…)



WPA(2) (*Wi-Fi Protected Access (II)*) **(nastavak)**

- **EAP** - *Extensible Authentication Protocol*
  - ako se pojavi novi klijent u mreži autentikator mu otvori port, koji je u neautoriziranom stanju
  - autentikator pošalje EAP zahtjev prema korisniku
  - korisnik odgovara EAP odgovorom
  - autentikator prosljeđuje EAP odgovor prema poslužitelju za autentikaciju
  - ako poslužitelj za provjeru vjerodostojnosti prihvati zahtjev, autentikator njegov port stavlja u stanje dozvoljenog pristupa
  - kada korisnik dobije pristup, dozvoljen mu je normalan promet

WPA(2) (*Wi-Fi Protected Access (II)*) (nastavak)

- **EAP-TLS** – *EAP Transport Layer Security*
  - izvorno zamišljeno kao dio Windows XP operacijskog sustava
  - cilj je osiguravanje sigurne komunikacije između klijenta i servera
  - umjesto šifri oslanja se na uporabu certifikata
  - problem certifikata je fizička krađa uređaja i njihova uporaba bez poznavanja šifre, a prednost je veća sigurnost pri pokušaju napada
- **EAP-TTLS** – *EAP Tunneling Transport Layer Security*
  - zahtijeva se provjera vjerodostojnosti poslužitelja prije provjere vjerodostojnosti klijenta
  - sigurni “tunel” stvara se na transportnom sloju u komunikaciji između korisnika i poslužitelja uporabom TLS-a
  - provjera vjerodostojnosti se obavlja preko uspostavljenog zaštićenog tunela

WPA(2) (*Wi-Fi Protected Access (II)*) **(nastavak)**

- **EAP-PEAP** – *Protected Extensible Authentication Protocol*
  - izgovara se "peep"
  - razvili su ga Cisco, Microsoft i RSA Security
  - sličan je EAP-TTLS-u jer također stvara tunel prilikom provjere vjerodostojnosti
  - koristi PKI certifikat koji se nalazi na serveru
  - 2 podvrste od 2005. godine:
    - **PEAPv0/EAP-MSCHAPv2**: najčešći oblik PEAP-a
    - **PEAPv1/EAP-GTC**: kreirao ga je Cisco, ne podržava ga Windows operacijski sustav

Zaštita WLAN mreža

- možemo govoriti o različitom stupnju zaštite za kućne i korporacijske WLAN mreže
- kod kućnih WLAN mreža najčešće se potrebno zaštititi od napadača koji imaju za cilj “besplatan” pristup Internetu, a rijetko krađu osobnih podataka
  - dovoljno je korištenje WPA(2) sustava
  - MAC filtriranje također je česta opcija
  - SSID skrivanje još je jedan od učinkovitih načina zaštite
- kod korporacijskih WLAN mreža, napadači često žele doći do povjerljivih podataka, pa sam sustav zaštite mora biti robusniji
  - najčešće se koristi WPA(2) poslužiteljem RADIUS za provjeru vjerodostojnosti

MAC filtriranje

- **MAC** – *Media Access Control*
  - MAC adresa je jedinstven identifikator mrežnog sučelja
  - zapisana je u ROM uređaja
  - sastoji se od 6 parova heksadecimalnih znamenki (48 bita)
  - teoretski je moguće adresirati 2^{48} uređaja (281.474.976.710.656)
  - primjer MAC adrese je: 00-0C-F1-56-98-AD
    - 00-0C-F1 označavaju proizvođača (Intel)
    - 56-98-AD dodjeljuje proizvođač
- pristup ograničavanjem na određene MAC adrese nije naročito učinkovit način zaštite mreža
- ovakav tip zaštite predstavlja problem kod mreža s čestom izmjenom računala, jer je potrebno dodavati nove adrese u MAC tablice pristupa

SSID skrivanje

- **SSID** – *Service Set IDentifier*
  - ime koje određuje pojedinu WLAN mrežu
  - može imati do 32 znaka (okteta)
  - korisnik s administratorskim ovlastima može kreirati proizvoljni SSID
  - omogućeno je da dvije ili više pristupnih točki odašilju isti SSID ukoliko pripadaju istoj mreži
- skrivanje SSID-a, odnosno naziva mreže, pomaže kao dodatni zaštitni mehanizam
- prvenstveno se smanjuje vjerojatnost napada onih koji ne znaju da ta mreža postoji
- napadač koji zna za mrežu, bez obziran na skrivanje SSID-a s jednakom vjerojatnošću će ostvarit cilj svog napada kao da se SSID odašilje

Napad na WLAN mreže

- ometanje radijskim signalom postiže se pomoću odašiljača ometača (*jammer*) koji radi na istoj frekvenciji kao i radijska mreža
- princip na kojem odašiljač ometač radi je maskiranje korisnog signala smetajućim – uskraćivanje usluge bez krađe podataka

Odašiljač za ometanje WLAN i Bluetooth signala koji radi na frekvenciji od 2,4 GHz

Napad na WLAN mreže

- napad na slabo zaštićene WLAN mreže u svrhu korištenja usluga ili pristupa informacijama ostvariv je ovisno o stupnju zaštite mreže
- uglavnom je moguće probijanje samo WEP zaštite
- postoji mnogo alata koji omogućavaju probijanje
  - primjer **Kali Linux**

Zaštita kućnih WLAN mreža - zaključak

- teže je štititi WLAN od LAN mreža
- WEP je prvi algoritam zaštite radijske mreže od napada
- velik broj kućnih mreža i danas je zaštićen WEP-om iz razloga što je WEP postavio davatelj usluge kao tvorničku postavku
- IEEE 802.11i je standard zaštite koji objedinjuje autentikacijske protokole, upravljanje ključevima za kontrolu pristupa i algoritme za kriptiranje podataka
- WPA(2) zaštita daje gotovo potpunu sigurnost
- problem koji ostaje neriješen je ometanje odašiljačem koji radi na frekvenciji na kojoj je propisano korištenje WLAN-a, pri čemu ne dolazi do krađe podataka, već do onemogućavanja korištenja sustava