SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 9:

Sigurnost bežičnih i mobilnih mreža

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Sigurnost bežičnih i mobilnih mreža

- Sadržaj poglavlja i predavanja:
  - 9.1 Uvod u bežične mreže
  - 9.2 WEP
  - 9.3 802.1x, EAP, WPA, 802.11i i drugi standardi
  - 9.4 Alati za napadanje bežičnih mreža i dodatne reference
  - 9.5 Sigurnost GSM mreža
  - 9.6 *Bluetooth* sigurnost

Quote

To be happy in this world, first you need a cell phone and then you need an airplane. Then you're truly wireless.

—Ted Turner

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

Sigurnost bežičnih i mobilnih mreža

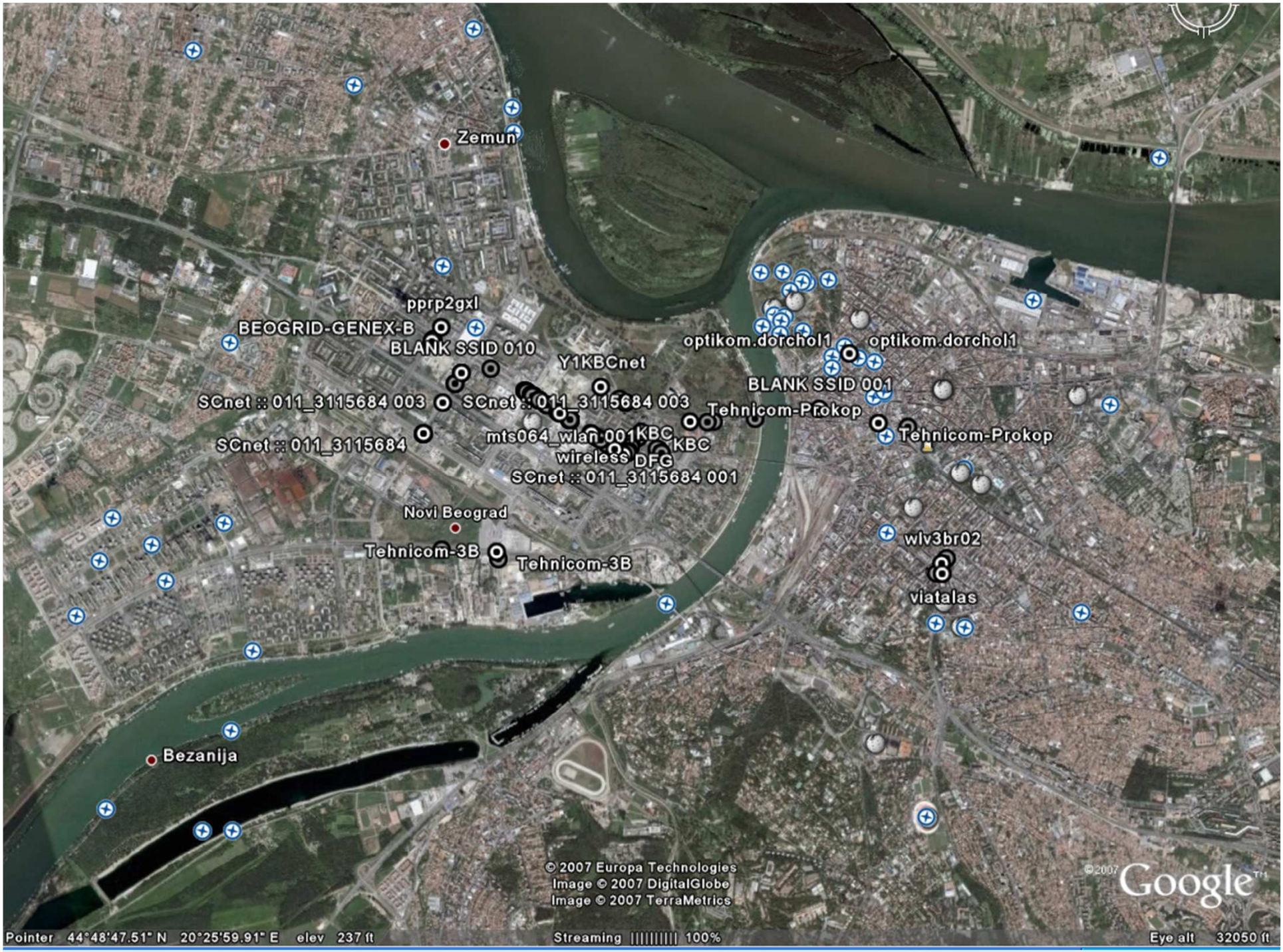
- Eksplozivan rast bežičnih (engl. *wireless*) i mobilnih mreža podseća na ekspanziju Interneta u devedesetim godinama prošlog veka.
- Zbog svih prednosti koje donose bežične mreže, one su danas masovno upotrebljavaju
- Trend postavljanja tzv. „vrućih“ tačaka (engl. *hot spots*)
- Mogućnost *roaminga* je posebno korisna i često upotrebljavana.

- Međutim, primena bežičnih mreža donela je sa sobom i brojne probleme u pogledu narušavanja sigurnosti i privatnosti.
- Propagacija signala bežične mreže stvara probleme zbog nemogućnosti jasnog određivanja perimetra (granice) mreže, a pojavljuju se i različite nove pretnje i napadi na sigurnost računarskih sistema i mreža specifični za ove vrste mreža.

Beograd - WarDriving

- Screenshoot Belgrad.kmz –> GoogleEarth + NetStumbler
- www.netstumbler.org
- www.netstumbler.com

- Alati:
  - Laptop sa 802.11a/b/g/n karticom
  - GPS
  - Netstumbler
  - Aircrack (ili neki drugi WEP *cracking tool*)
  - Ethereal
  - Automobil po izboru


Zemun
pprp2gxl
BEOGRID-GENEX-B
BLANK SSID 010
Y1KBCnet
optikom.dorchol1
optikom.dorchol1
BLANK SSID 001
SCnet :: 011_3115684 003
SCnet :: 011_3115684 003
Tehnicom-Prokop
Tehnicom-Prokop
SCnet :: 011_3115684
mts064_wlan 001KBC
KBC
wireless DFG
SCnet :: 011_3115684 001
Novi Beograd
wlv3br02
Tehnicom-3B
Tehnicom-3B
viatalas
Bezanija
© 2007 Europa Technologies
Image © 2007 DigitalGlobe
Image © 2007 TerraMetrics
© 2007 Google
Pointer 44°48'47.51" N 20°25'59.91" E elev 237 ft
Streaming 100%
Eye alt 32050 ft

9.1 Uvod u bežične mreže

- Bežične mreže su definisane standardom IEEE 802.11 koji je doneo IEEE (*Institute of Electrical and Electronics Engineers*).
- Standard definiše najniža dva sloja OSI modela: fizički i sloj veze.
- On je samo deo veće porodice standarda koji definišu lokalne (LAN) i gradske mreže (MAN).

Radne grupe za IEEE 802.11 standarde

- Grupa „**A**“ - zadužena za unapređenje inicijalnog standarda
- Grupa „**B**“ - zadužena za izradu bržeg DSSS prenosa na 2,4 GHz
- Grupa „**D**“ - zadužena za usklađivanje međunarodnih pravilnika o slobodnim radio-frekvencijama
- Grupa „**E**“ - koja obrađuje kvalitet servisa (QoS)
- Grupa „**F**“ - koja razrađuje podršku za roming
- Grupa "**G**" - zadužena za rad na 54 Mbps za zahtevne korisnike standarda 802.11b

- IEEE 802.11**n** is an amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4GHz and the lesser used 5 GHz bands. The IEEE has approved the amendment and it was published in October 2009. Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

Wi-Fi

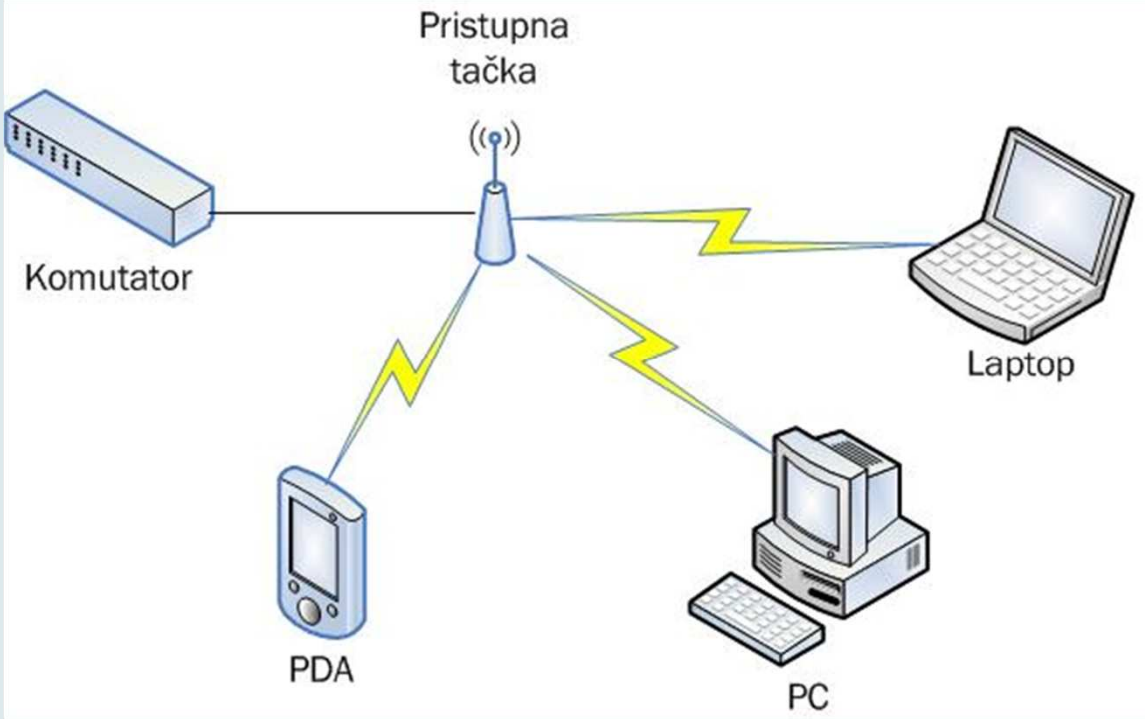
- Wi-Fi (takođe: WiFi, wifi i slično) trgovačka je marka (brend) koju je originalno licencirala organizacija Wi-Fi Alliance®

Infrastrukturne i *ad-hoc* mreže

- Većina bežičnih LAN mreža rade u takozvanom „infrastrukturnom“ režimu u kome pristupne tačke obezbeduju vezu bežičnih klijenata sa LAN mrežom. Standard definiše ovaj tip mreže kao *Basic Service Set* (BSS). Pristupne tačke (engl. *access points*) jesu uređaji preko kojih klijenti mogu dobiti pristup mreži. Prednost ovoga rešenja leži u tome što dopušta veću fleksibilnost u radu, veće domete signala i bolji kvalitet.

- „*Ad hoc*” režim, u kome bežične mrežne kartice rade nezavisno od pristupne tačke. Ovaj režim rada omogućava, na primer, korisnicima prenosnih računara (engl. *laptop*) da razmene datoteke, ili oforme radnu grupu bez ikakvih instaliranih kablova i druge komplikovane mrežne opreme. Standard definiše ovaj način povezivanja kao *Independent Basic Service Set* (IBSS).

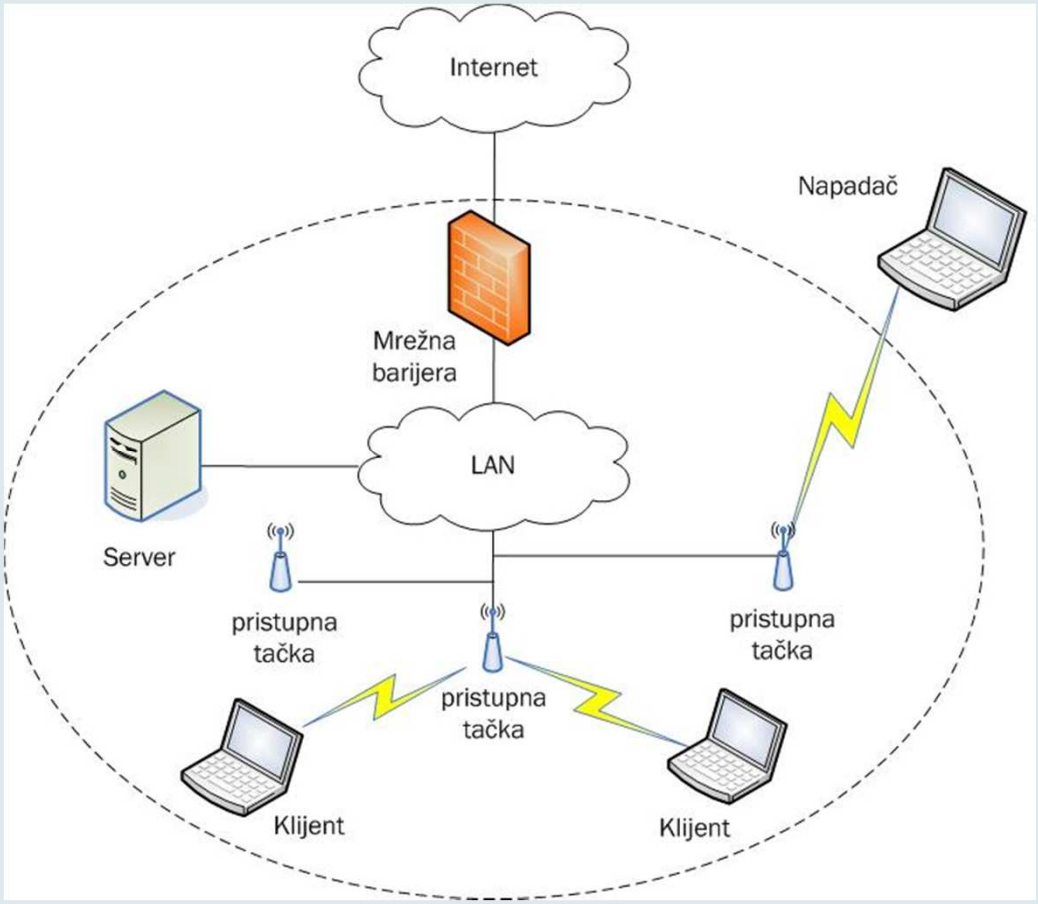
Infrastrukturne mreže



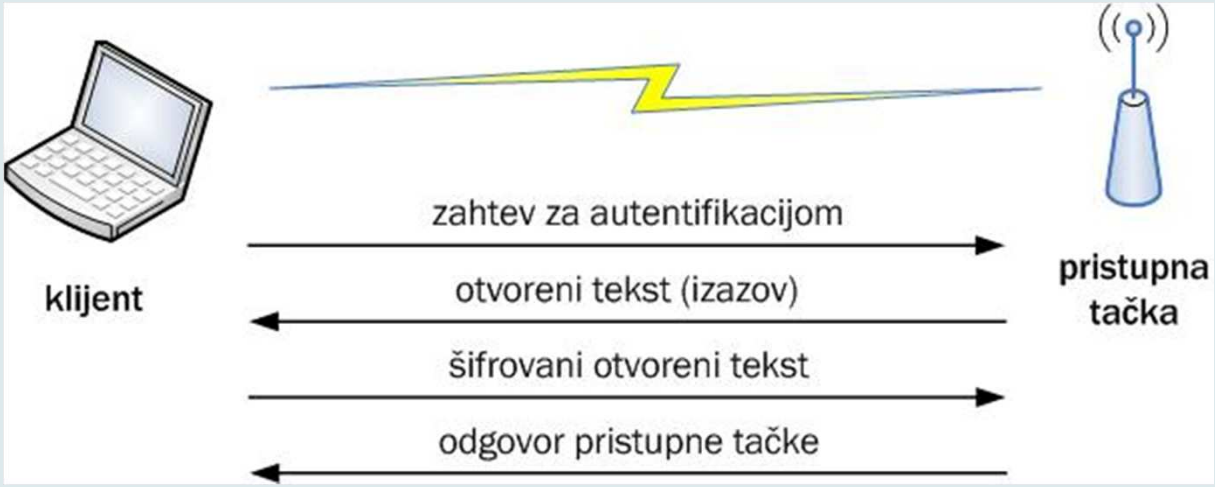
Bežične mreže i sigurnost

- Fizičko ograničavanje propagacije signala
- Identifikator skupa usluga (*Service Set Identifier, SSID*)
- Provera identiteta korisnika mreže
  - Provera identiteta otvorenog sistema (*Open System Authentication*)
  - Provera identiteta zasnovana na deljenoj tajni (*Shared Key Authentication*)

„Napad sa parkirališta“(engl. *parking lot attack*)



Provera identiteta zasnovana na deljenoj tajni

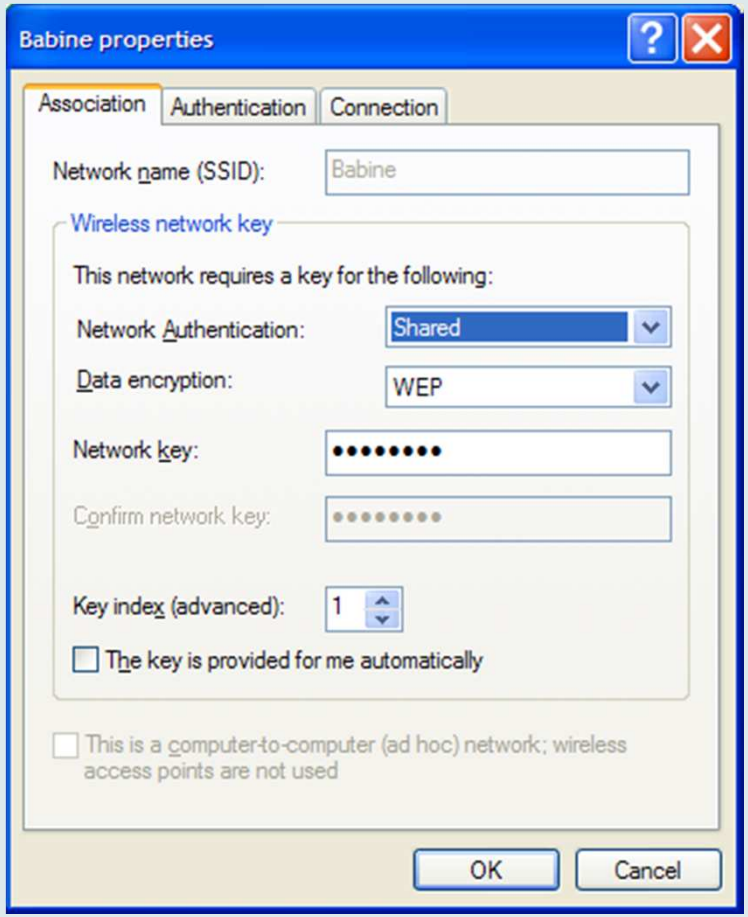


9.2 WEP

- **WEP** (***W****ired* ***E****quivalent* ***P****rivacy*) je definisan u standardu 802.11 i cilj mu je da obezbedi sledeće:
  - **Poverljivost poruka** – osnovna namena je spečavanje prisluškivanja mrežnog saobraćaja (engl. eavesdropping),
  - **Kontrolu pristupa** – pristupne tačke mogu zabraniti klijentima pristup mreži ukoliko ne zadovolje proveru uidentiteta, integritet poruka – dodatno polje u okviru služi za proveru integriteta samog okvira.

- WEP se koristi radi zaštite podataka na sloju veze OSI modela.

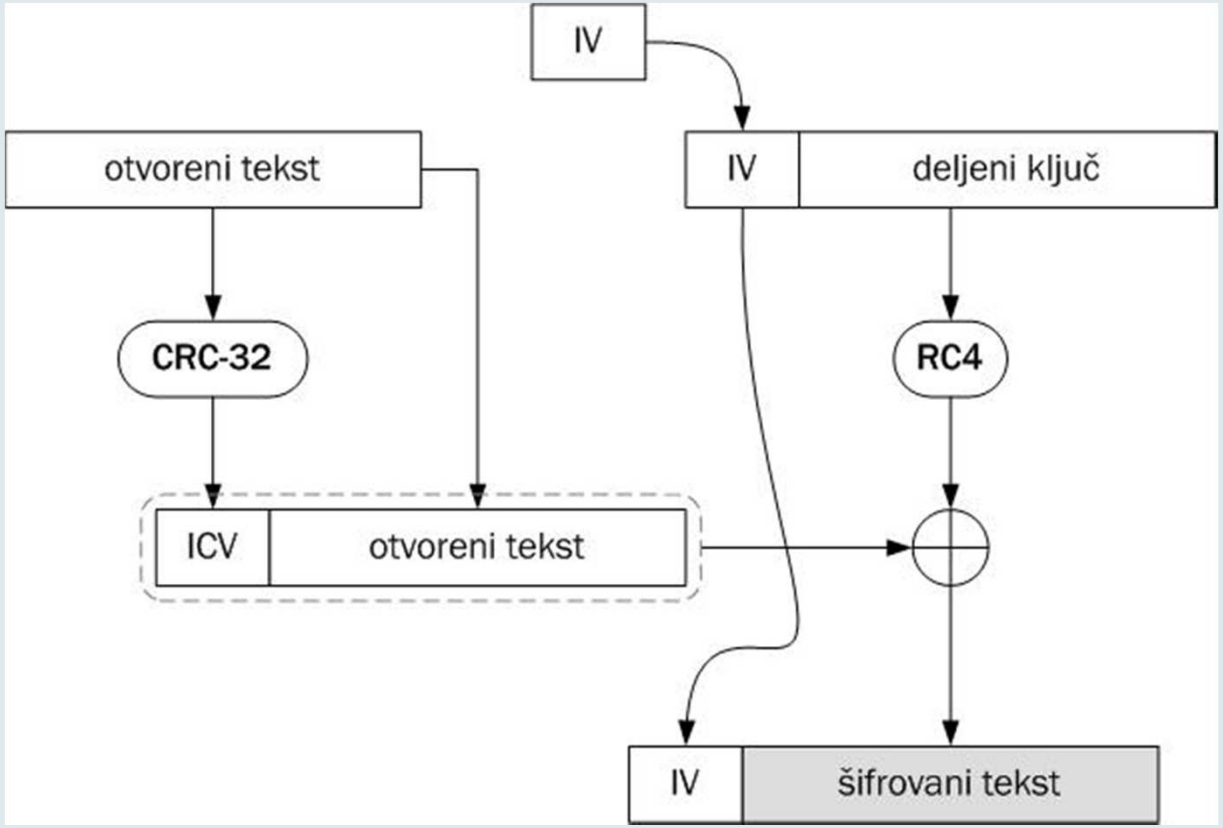
Dijalog “Wireless Network Properties”



WEP šifrovanje

- Za šifrovanje tela okvira koristi se simetričan protočni algoritam RC4.
- Algoritam generiše veliki broj pseudoslučajnih bitova kao funkciju ključa *k* i inicijalizacionog vektora *IV*.
- Ovaj niz bitova označava se sa *RC(IV,k)*.
- Posle toga se vrši operacija ekskluzivno ILI nad bitovima otvorenog teksta i dobijenim nizom pseudoslučajnih bitova kako bi se dobio šifrovani tekst.

Šematski prikaz standardnog WEP šifrovanja i dobijanja WEP okvira



Sigurnosni propusti u WEP standardu

- Prilikom komunikacije klijenta i pristupne tačke, podaci se šalju u obliku kontrolnih okvira čija zaglavlja nisu šifrovana, što znači da napadač lako može doći do inicijalizacionog vektora koji je korišćen za šifrovanje. Napadač koji "uhvati" dva šifrata šifrovana istim inicijalizacionim vektorom dobiće informacije o samim porukama.
- Pošto zamena ključa nakon svakog poslatog okvira nije moguće rešenje ovog problema, WEP standard preporučuje (ali ne insistira) da se nakon svakog okvira promeni inicijalizacioni vektor. Mnogi proizvođači mrežne opreme slede ovu preporuku, ali su neki to učinili na veoma loš način. Na primer, većina PCMCIA bežičnih mrežnih kartica prilikom svakog pokretanja postavlja inicijalizacioni vektor na nulu i povećava ga za jedan nakon svakog poslatog okvira. Napadaču je u tom slučaju dovoljno da zna samo deo vektora sa početka i na taj način može doći do nekih podataka.
- Dodatno, u arhitekturi WEP-a postoji propust koji pogađa sve implementacije protokola i time izlaže korisnika ozbiljnoj opasnosti ponovne upotrebe ključa. Polje u kojem je upisana vrednost inicijalizacionog vektora dugačko je 24 bita, što znači da postoji 2^{24}=16.777.216 različitih vrednosti tog vektora. Ukoliko se uzme u obzir činjenica da će prosečna stanica koja šalje okvire veličine 1500 bajtova pri prosečnoj brzini od 5 Mbps iscrpeti sve vektore za manje od pola dana, jasno je da je ovo ozbiljan propust.

Napadi na WEP

- Postoji nekoliko vrsta napada na WEP, a oni se grubo mogu klasifikovati u dve kategorije:
  - **Pasivni napadi** – napadač samo prisluškuje komunikaciju korisnika sa mrežom. U ove napade spadaju analiza mrežnog saobraćaja i pasivno prisluškivanje;
  - **Aktivni napadi** – napadač aktivno utiče na mrežni saobraćaj ubacivanjem svojih podataka, lažiranjem komunikacije između klijenta i pristupne tačke, zagušivanjem saobraćaja na mreži ili neovlašćenim korišćenjem mrežnih resursa. U ove napade spadaju ponavljanje inicijalizacionog vektora, obrtanje bitova, čovek u sredini, krađa sesije i napad ponavljanjem paketa.

Pasivni napadi

- Nadziranje i analiza mrežnog saobraćaja
- Pasivno prisluškivanje

Ostali napadi

- Napad ponavljanjem inicijalizacionog vektora
- Napad obrtanjem bitova
- Napad „čovek u sredini“
- Krađa sesije (engl. *session hijacking*)
- Napad ponavljanjem paketa (engl. *packet re-play attack*)

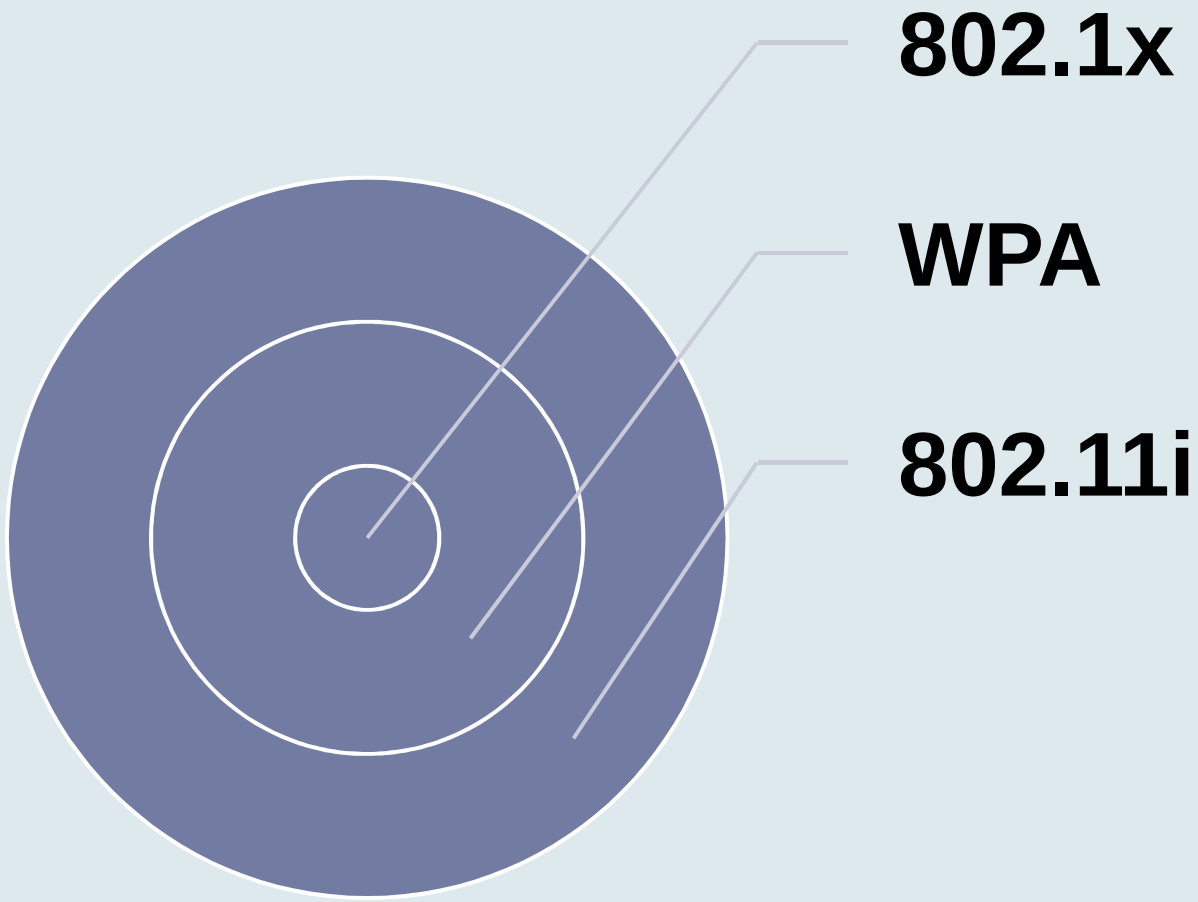
Upravljanje ključevima

- Standard definiše dve metode za korišćenje WEP ključeva.
  - Prvi metod dozvoljava prozor sa četiri ključa.
  - Drugi metod je mapiranje ključeva (engl. *key mapping method*). U ovom metodu, svaka jedinstvena MAC adresa može imati svoj ključ.

Demo

- Whoppix-WEP-crack.avi

Odnos između sigurnosnih standarda



WEP2

- WEP2 je još jedan u nizu pokušaja povećanja sigurnosti bežičnih mreža. Kao što se iz imena standarda može naslutiti, on je nastao kao nadogradnja WEP-a, što znači da je nasledio neke fundamentalne slabosti u dizajnu. IEEE menja dužinu ključa sa 40 na 128 bitova i proširuje polje u kome se nalazi inicijalizacioni vektor sa 24 na 128 bitova. Takođe, WEP2 podržava protokol Kerberos V.
- Algoritam za šifrovanje i način upravljanja ključevima nisu izmenjeni, što znači da WEP2 ne donosi veliki pomak u povećanju sigurnosti. Dobra osobina je to što je WEP2 kompatibilan sa WEP protokolom, što znači da postojeća mrežna oprema - uz određenu programsku nadogradnju - može koristiti WEP2.

9.3 802.1x, EAP, WPA, 802.11i i drugi standardi

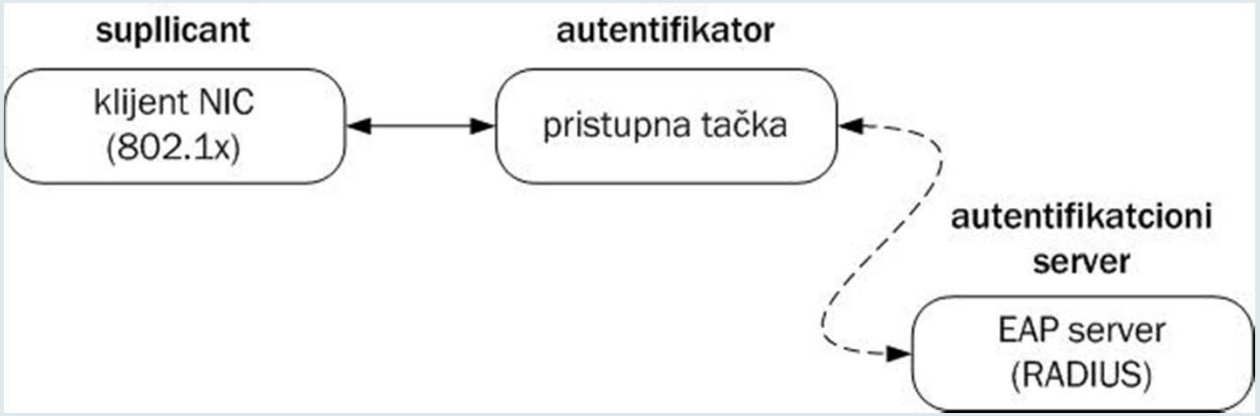
- IEEE je, uočivši propuste u standardu, započeo rad na novim predlozima i rešenjima kako bi se povećala sigurnost bežičnih mreža. Tako je nastao standard 802.1x.
- Fokus standarda 802.1x je unapređenje mehanizma provere identiteta, čime se rešava dobar deo trenutnih problema sigurnosti bežičnih mreža.
- 802.1x radi na MAC podsloju drugog sloja OSI modela. Klijenti se pridružuju mreži preko portova, koji u okvirima standarda označavaju pridruživanje klijenata pristupnoj tački.
- Standard 802.1x pruža radni okvir (engl. *framework*) za različite metode provere identiteta – pomoću lozinki, sertifikata i pametnih kartica (engl. *smartcard*).

IEEE 802.1x

- IEEE 802.1x apstrahuje tri entiteta:
  - klijenta – tj. molioca (engl. *supplicant*),
  - autentifikatora i
  - server za proveru identiteta.

- Molilac (mrežna kartica klijenta) koristi usluge autentifikatora (pristupne tačke) koje mu on nudi preko portova. Klijent se posredstvom autentifikatora predstavlja serveru za proveru identiteta (bilo koji EAP server, najčešće RADIUS) koji nalaže autentifikatoru da *supplicantu* dozvoli pristup mreži. Pretpostavka je da svi autentifikatori komuniciraju sa istim centralnim servisom za proveru identiteta.

Entiteti standarda 802.1x



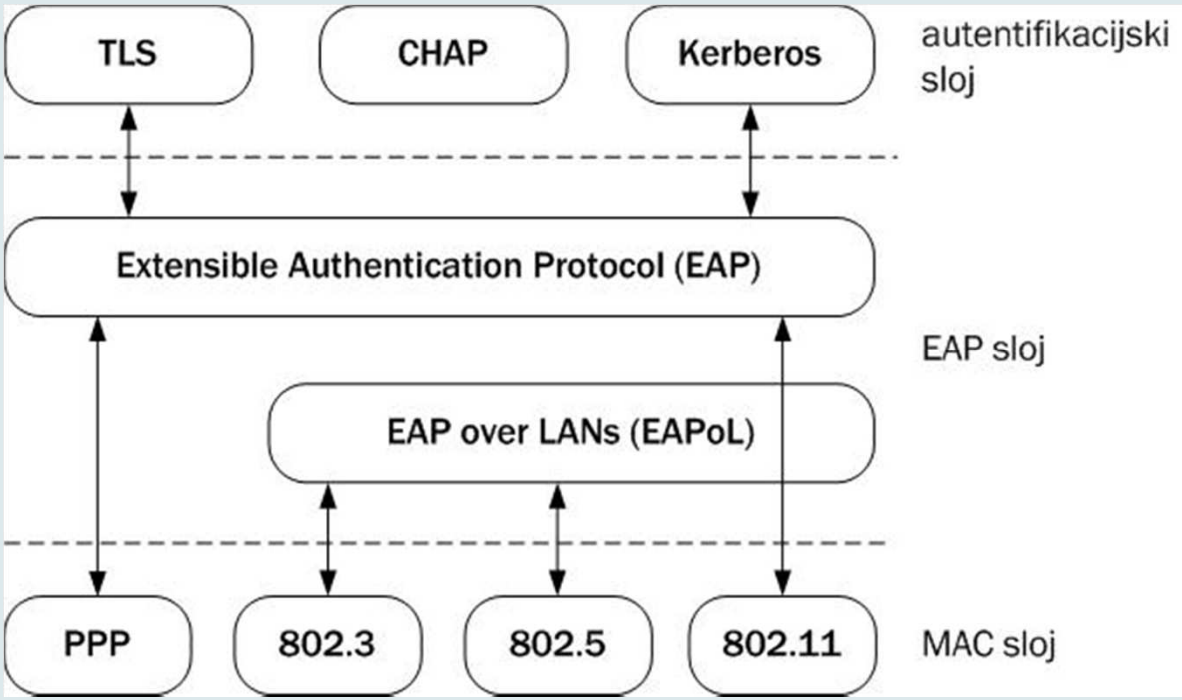
EAP

- Standard 802.1x koristi EAP (*Extensible Authentication Protocol* kao osnovu za korišćenje različitih mehanizama za proveru identiteta. EAP je izgrađen na osnovu paradigme izazov-odgovor (engl. *challenge-response*). Prvobitno je bio namenjen za upotrebu u "žičanim" mrežama, ali je kasnije implementiran i u bežičnim. EAP radi na drugom sloju OSI modela.

- U protokolu EAP postoje četiri osnovna tipa poruka:
  - *EAP Request* – izazov koji autentifikator šalje moliocu,
  - *EAP Response* – odgovor molioca autentifikatoru,
  - *EAP Success* – autentifikator prihvata molioca,
  - *EAP Failure* – autentifikator odbija molioca.

- U bežičnoj mreži, EAP paket se enkapsulira u EAPoL (*EAP over LANs*). EAPoL paketi služe za komunikaciju između molioca i autentifikatora preko mreže. Postoje tri vrste EAPoL paketa:
  - *EAPoL Start* – nalaže autentifikatoru da počne proces provere identiteta,
  - *EAPoL Logoff* – obaveštava autentifikatora da se korisnik odjavljuje s mreže,
  - *EAPoL Key* – nosi informaciju o WEP deljenom ključu.

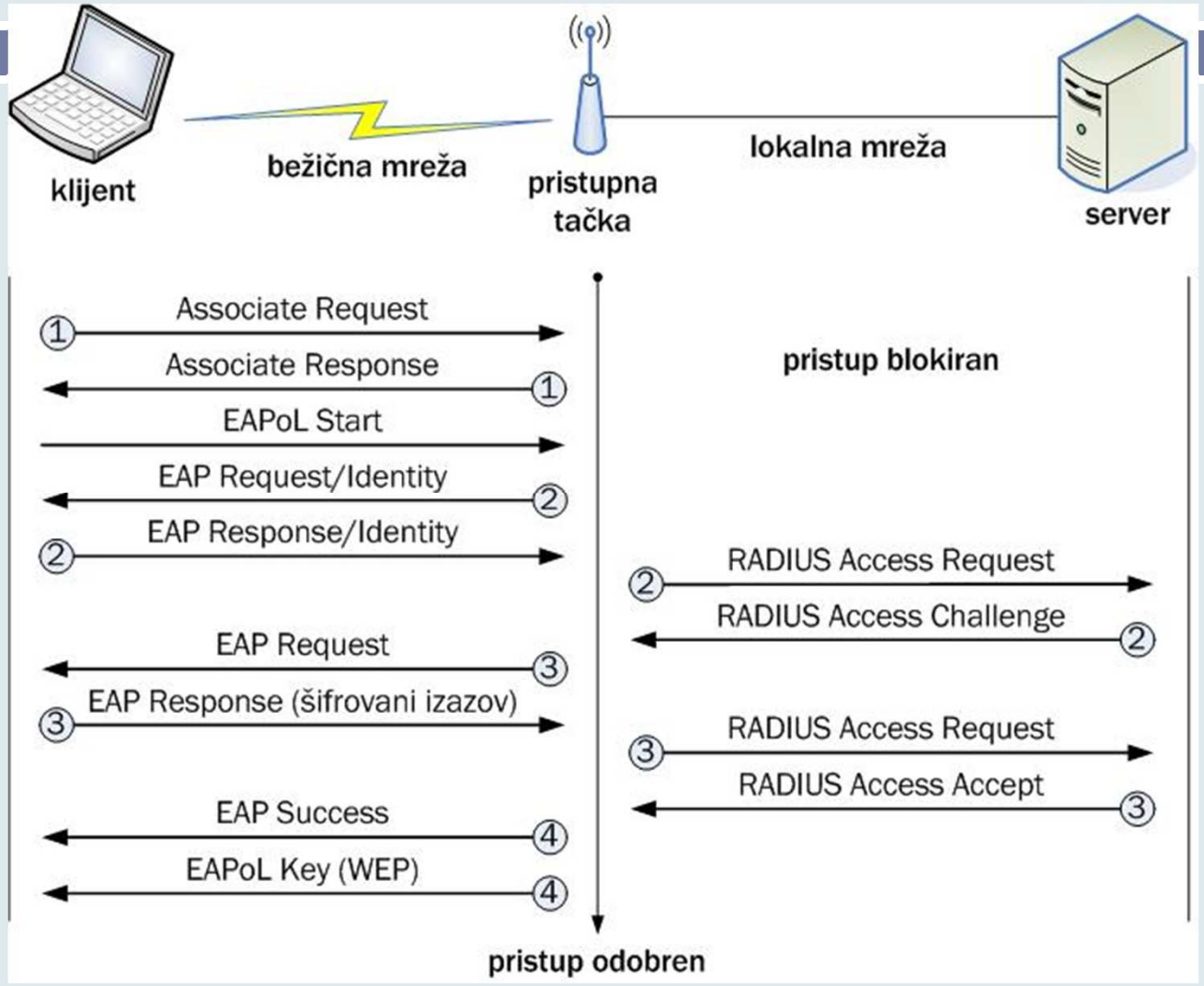
EAP stek



EAP…

- EAP je proširiv u smislu da se unutar EAP zahteva i odgovora može enkapsulirati bilo koja metoda provere identiteta. EAP može da preusmeri sve zahteve za proverom identiteta ka centralnom RADIUS serveru.
- Kako bi korisnik mogao da pristupi mreži, pristupna tačka mora da omogući EAP paketima da prođu do servera. Zbog toga autentifikator koristi dualni način rada portova. Portovi mogu biti:
  - nekontrolisani (engl. *uncontrolled ports*) i
  - kontrolisani (engl. *controlled ports*).
- Nekontrolisani portovi ne dopuštaju nikakav drugi saobraćaj osim EAP paketa. Ovaj model je kompatibilan sa klijentima koji ne podržavaju standard 802.1x. Naime, administrator može saobraćaj između takvih klijenata preusmeriti na nekontrolisane portove i time im omogućiti pristup mreži.

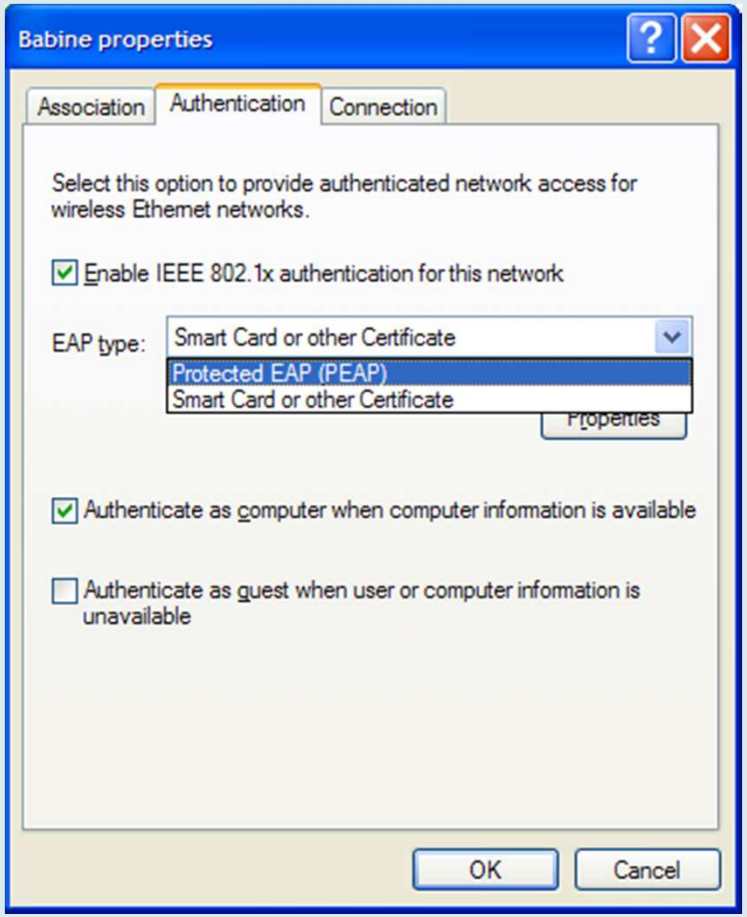
Provera identiteta po protokolu EAP



Vrste EAP-a

- EAP MD5
- EAP TLS (*Transport Layer Security*)
- EAP TTLS (*Tunneled Transport Layer Security*)
- PEAP (*Protected Extensible Authentication Protocol*)
- EAP LEAP (*Light Extensible Authentication Protocol*)
- EAP SIM (*Subscriber Identity Module*)
- EAP AKA (*Authentication and Key Agreement*)

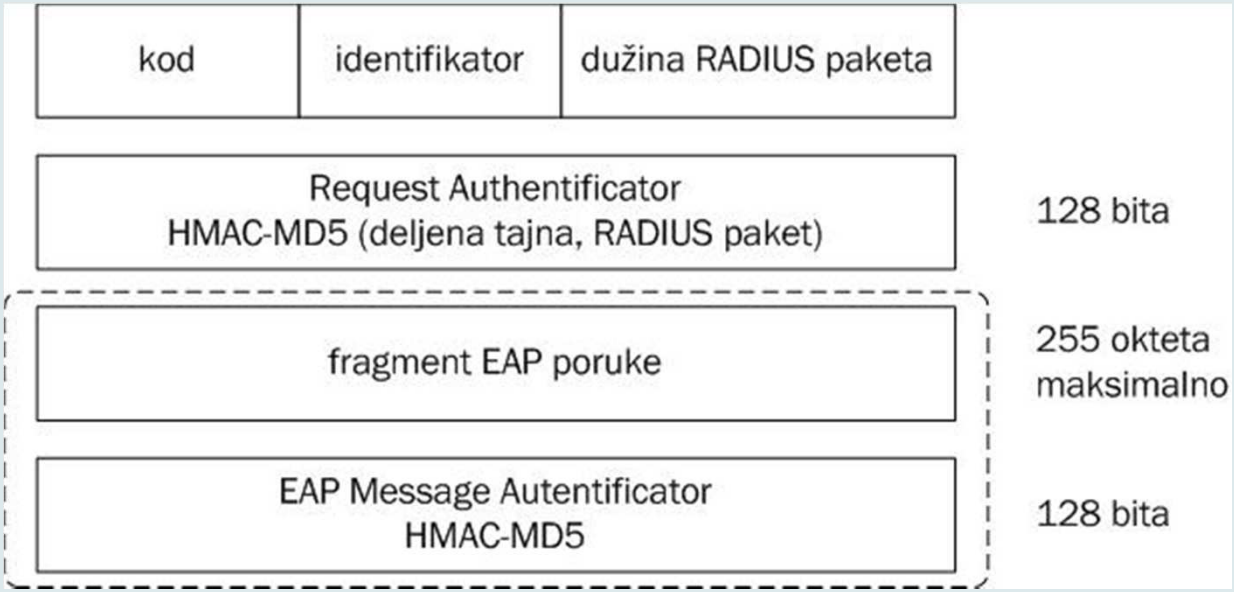
Biranje PEAP protokola za proveru identiteta



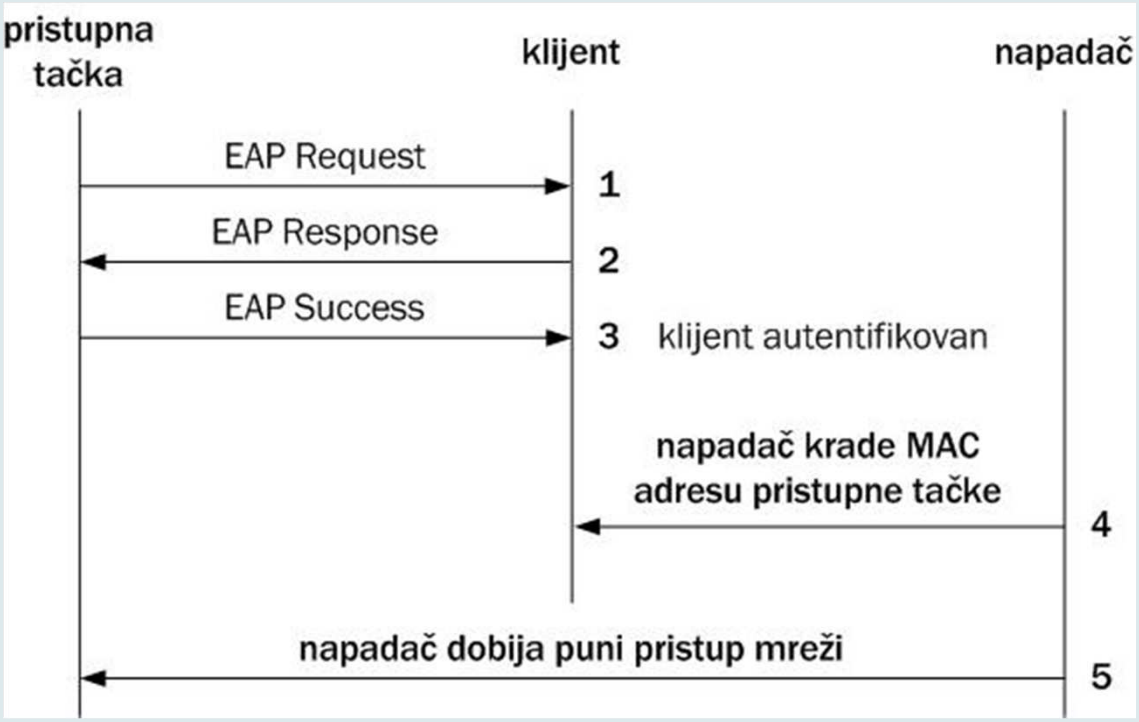
Sigurnosni ciljevi standarda 802.1x

- Kontrola pristupa i mogućnost međusobne provere identiteta
- Fleksibilnost i skalabilnost
- Sigurnost
- Stroga poverljivost podataka

RADIUS paket



Sigurnosni propusti i napadi na 802.1x i krađa sesije



Poboljšanja 802.1x

- Simetrična provera identiteta
- Skalabilna provera identiteta

- Ostalo:
  - Korišćenje IPSec protokola u bežičnim mrežama

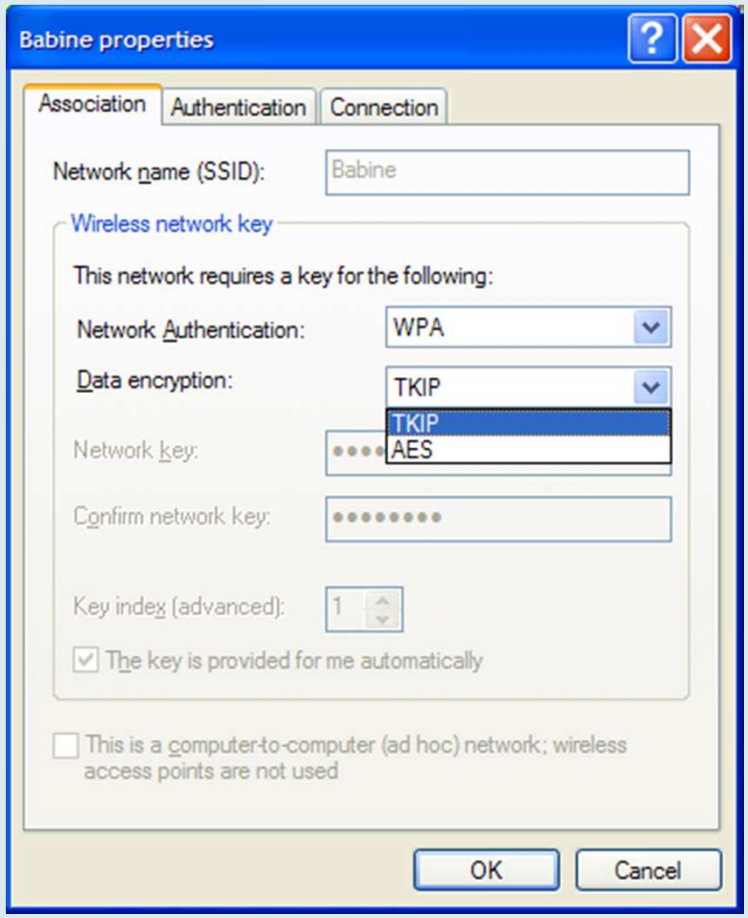
Novi standardi bežičnih mreža

- WPA (*Wi-Fi Protected Access*)
- WPA2
- IEEE 802.11i

WPA

- WPA koristi:
  - TKIP protokol (*Temporal Key Integrity Protocol*) za šifrovanje,
  - Standard 802.1x i neki od uobičajenih EAP protokola za proveru identiteta,
  - MIC (*Message Integrity Check*, pominje se i pod imenom "*Michael*") za sprečavanje lažiranja paketa

Biranje WPA provere identiteta i TKIP šifrovanja



WPA2

- WPA2 implementira obavezne elemente 802.11i standarda
- Dodatno, osim TKIP i Michael algoritma, uvodi novi AES bazirani algoritam CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) koji se smatra veoma sigurnim
- Od 13. marta 2006, WPA2 sertifikacija je obavezna za sve nove uređaje za koje se želi da budu Wi-Fi sertifikovani

IEEE 802.11i

- IEEE 802.11i je dodatak na 802.11 standard koji specificira sigurnosne mehanizme za bežične mreže (Wi-Fi).
- Radni standard je ratifikovan 24. juna 2004. i zamenjuje WEP koji se pokazao kao nesiguran.
- WPA implementira podskup 802.11i
- Wi-Fi Alliance referira na ovaj standard kao na WPA2
- 802.11i koristi AES, dok WEP i WPA koriste RC4 šifrovanje

- 802.11i arhitektura sadrži sledeće komponente:
  - 802.1X za proveru identiteta (engl. *authentication*) što povlači upotrebu EAP-a i autentifikacionog servera,
  - RSN (*Robust Security Network*) za držanje tj. praćenje asocijacija ("pridruživanja") i
  - AES bazirani CCMP da obezbedi tajnost, integritet i izvornu (originalnu) proveru identiteta.
  - Drugi važan element procesa autentifikacije je "*four-way handshake*"

IEEE 802.11i

- CCMP se smatra boljim i trajnijim rešenjem problema zaštite podataka u bežičnim mrežama. CCMP je zasnovan na AES algoritmu (*Advanced Encription Standard*) koji radi u takozvanom CCM režimu rada (*Counter Mode Encryption with CBC-MAC Data Origin Authenticity*). Upotreba CCMP-a je obavezna u svim implementacijama standarda 802.11i.

- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) je IEEE 802.11i protokol šifrovanja kreiran da zameni, zajedno sa TKIP, raniji nesigurni WEP protokol.

9.4 Alati za napadanje bežičnih mreža i dodatne reference

- Teorijska osnova koja leži iza takozvanih FMS (Fluhrer-Mantin-Shamir) tipova napada opisana je u članku „*Weaknesses in the Key Scheduling Algorithm of RC4*“ koji su objavili Scott Fluhrer, Itsik Mantin i Adi Shamir. Ovaj članak, koji se lako može naći na Internetu, pokrenuo je razne događaje vezane za napad na WEP ključ. Alati koji mogu razbiti WEP šifrovanje, a koji koriste slabosti inicijalizacionih vektora (IV) zovu se FMS alati (engl. *FMS utilities*).

- Airsnort
- WEP Crack
- AirCrack
- WEPwedgie
- Wi-Foo (www.wi-foo.com)
- ...

Moj doprinos

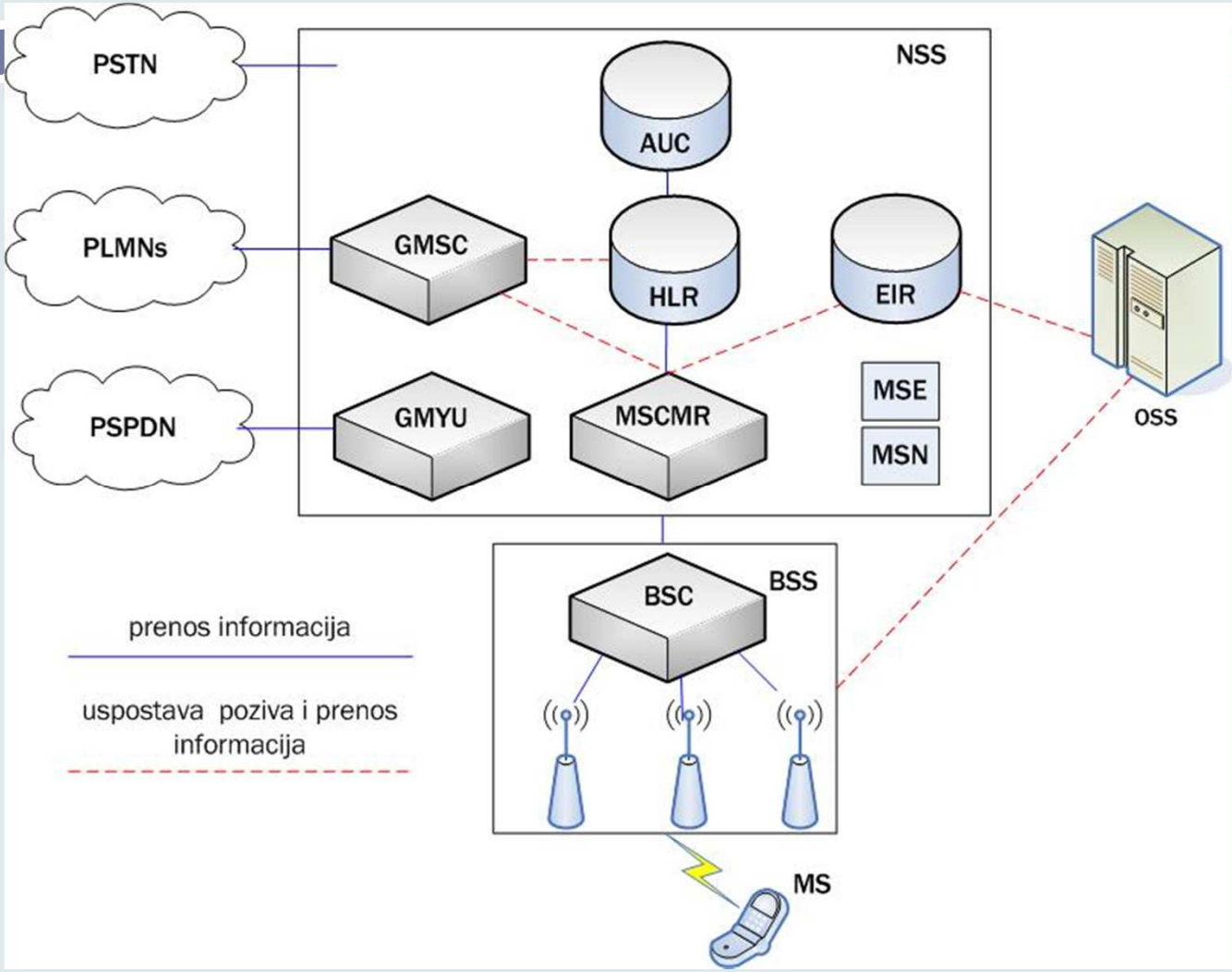
- Inicirao sam i radio na pokretanju projekta razvoja softverskog alata Wireless Roaming Client (www.pctel.com), koji koriste vodeće kompanije za pružanje usluga povezivanja na Wi-Fi i mobilne mreže (*WiFi, mobile and celluar providers*), omogućujući korisnicima povezivanje na bežične i mobilne (celularne) mreže preduzeća, vrućih tačaka (engl. *hot-spot*), kućnih mreža, mreža aerodroma, hotela, konferencijskih centara, kafića, restorana itd. Ovaj projekat je uključivao i razvoj i primenu različitih sigurnosnih mehanizama u bežičnim mrežama.

- Trenutno istraživanje WIDS / WIPS
- Itd...

9.5 Sigurnost GSM mreža

- GSM specifikacija identifikuje **tri sigurnosne usluge** od značaja za GSM komunikaciju:
  - **provera identiteta korisnika** – sposobnost mobilnog uređaja da dokaže da ima dozvolu za korišćenje određenog pretplatničkog računa kod GSM operatera,
  - **poverljivost podataka i signalizacionih paketa** – svi podaci (govor i tekstualne poruke) i signalizacioni paketi moraju biti šifrovani,
  - **anonimnost korisnika** – u trenutku provere identiteta pretplatnika, jedinstveni IMSI mora biti šifrovan.

GSM mreža



Provera identiteta korisnika

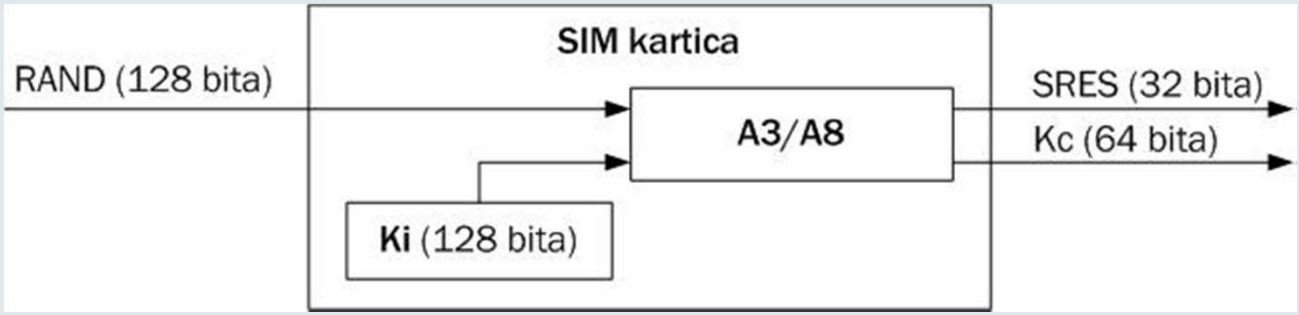
- IMEI (*International Mobile Equipment Identity*) - jedinstven petnaestocifreni broj koji se koristi za identifikaciju mobilnog uređaja u mobilnoj mreži. Utisnut je na unutrašnjoj strani mobilnog uređaja (kod baterije), a moguće ga je i očitati pozivom na *#06#. Sastoji se od tri polja:
  - *Type Allocation Code, TAC* – osmocifreni broj koji određuje zemlju porekla mobilnog uređaja i proizvođača
  - *Serial Number, SNR* – šestocifreni serijski broj uređaja
  - *Check Digit, CD* – kontrolni broj koji se koristi za proveru verodostojnosti IMEI broja na različitim tipovima mobilnih uređaja.

SIM kartica

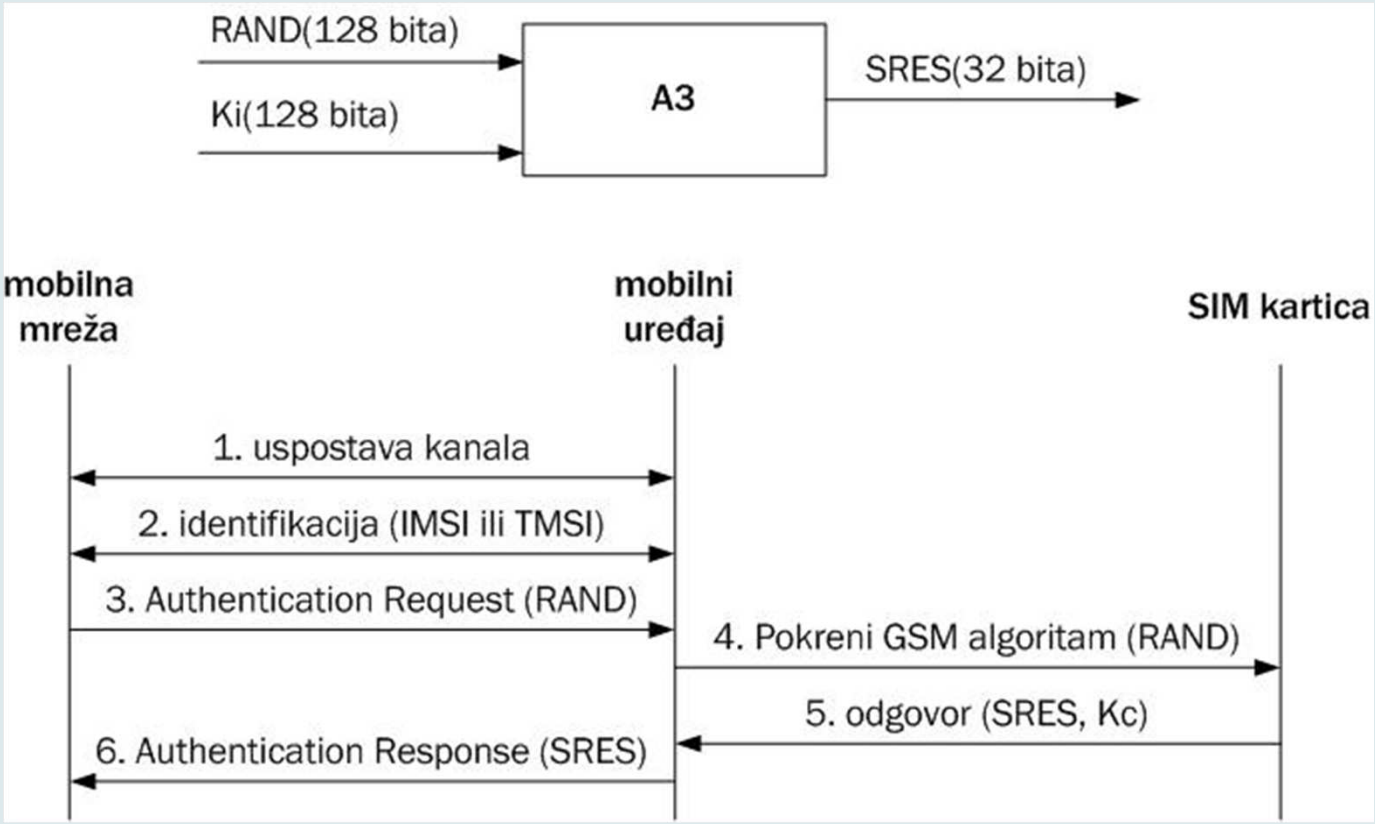
- **IMSI** (*International Mobile Subscriber Identity*) - jedinstven broj dodeljen svakom korisniku mobilnog uređaja (svakom pretplatniku) na svetu. Sadrži informacije o domaćoj mreži pretplatnika i zemlji u kojoj se nalazi ta mreža. Ova informacija se može dobiti samo lokalnim pristupom mobilnom uređaju, tj. SIM kartici, a najčešće je zaštićena samo PIN brojem (engl. *Personal Identification Number*). IMSI sadrži do 15 cifara, od kojih prvih 5 ili 6 specificira mrežu i zemlju operatera.

- **Korenski ključ** Ki (engl. *Root Encryption Key*). To je slučajno generisan 128-bitni broj dodeljen svakom pretplatniku, koji predstavlja početni ključ za generisanje svih provera tokom GSM komunikacije. Ključ Ki je strogo zaštićen i poznat je samo SIM kartici i mrežnom centru za proveru identiteta (AUC). Mobilni uređaj ne zna vrednost ključa Ki; uređaj daje SIM kartici samo informacije potrebne za proveru identiteta i generisanje ključeva za šifrovanje. SIM kartica sadrži mikroprocesor, tako da ona obavlja proveru identiteta i generisanje ključeva

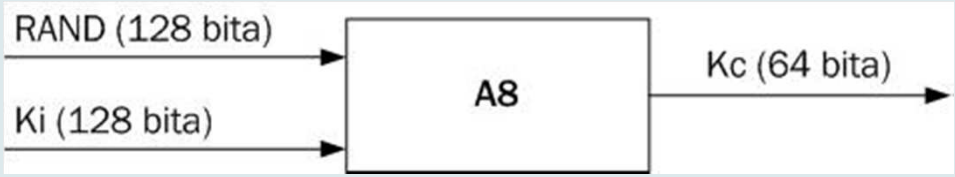
Koncept provere identiteta u SIM kartici



Algoritam A3 i provera identiteta

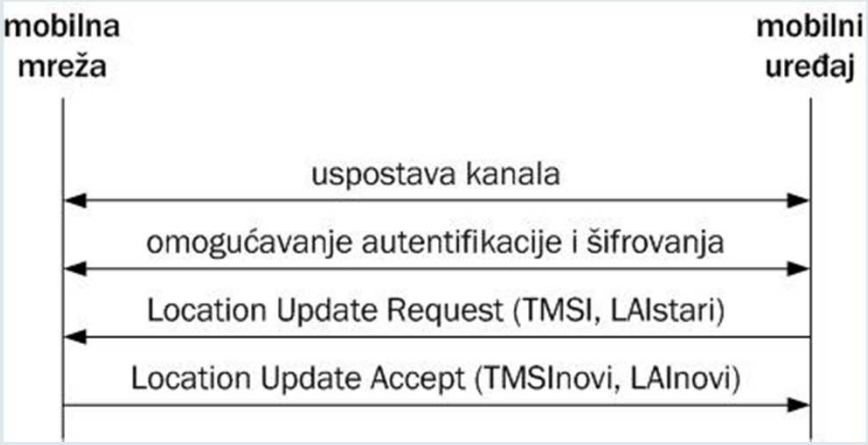


Šifrovanje komunikacije - Generisanje ključa za šifrovanje



Anonimnost korisnika

- Dodela novog TMSI broja (u slučaju promene lokaliteta)



- Dodela novog TMSI broja (u slučaju da nema promene lokaliteta)

Ostali sigurnosni problemi

- Više u o ovoj temi knjizi “Sigurnost računarskih sistema i mreža”
- Seminarski radovi

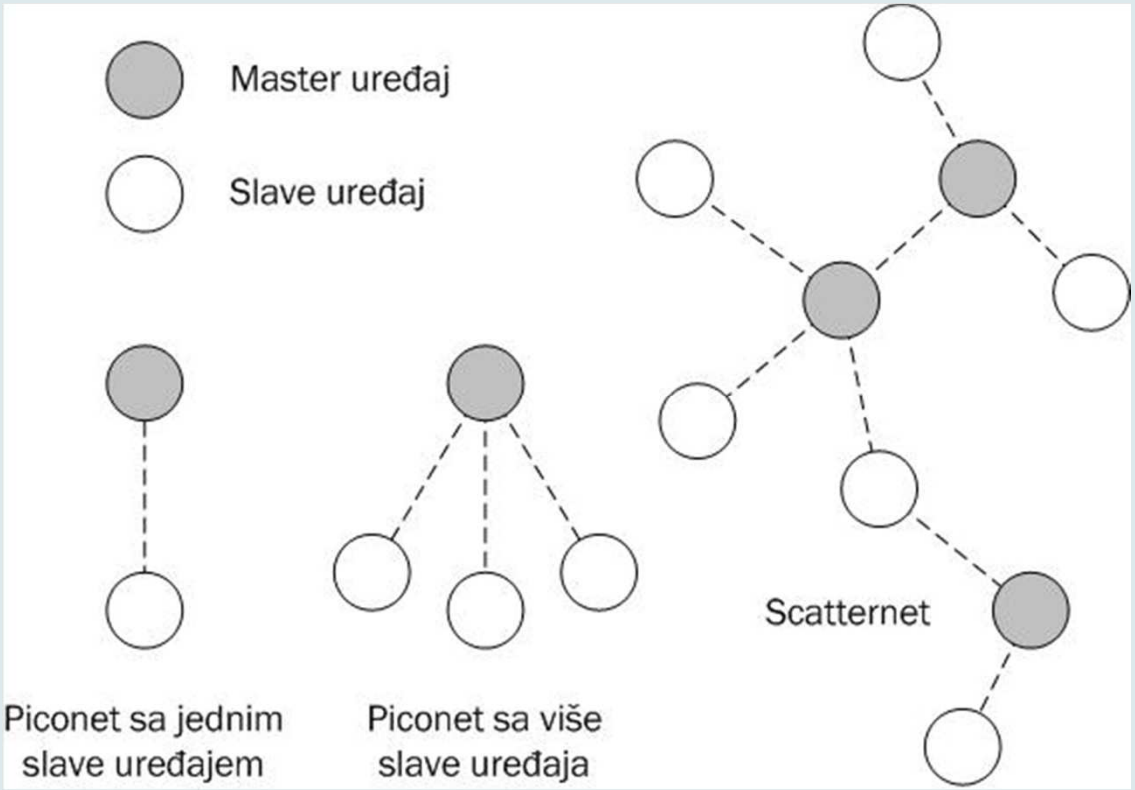
9.6 Sigurnost Bluetooth tehnologije

- Bluetooth je tehnologija namenjena bežičnim komunikacijama za kratke domete.
- Osnovna namena Bluetooth tehonologije je povezivanje različitih uređaja putem radio-talasa. Bluetooth je radio-veza kratkog dometa koja deluje na besplatnom ISM (*Industrial*, *Scientific*, *Medicine*) frekvencijskom opsegu 2,4 GHz (2400 MHz do 2483.5 MHz).

Bluetooth tehnologija

- Veze tipa:
  - tačka-tačka (engl. *point-to-point*)
  - tačka-više tačaka (engl. *point-to-multipoint*)
- Dva ili više uređaja koji dele zajednički kanal stvaraju ad hoc mrežu zvanu elementarna mreža (engl. *piconet*)
- Više elementarnih mreža koje deluju u istom području pokrivanja signala čine tzv. labavu mrežu (engl. *scatternet*).

Načini povezivanja Bluetooth uređaja…



Sigurnost Bluetooth komunikacije

- Postoje tri režima sigurnosti za Bluetooth pristup između dva uređaja.
  - sigurnosni režim 1 – nesiguran (engl. *non-secure*)
  - sigurnosni režim 2 – sigurnost nametnuta na nivou usluge (engl. *service level enforced security*)
  - sigurnosni režim 3 – sigurnost nametnuta na nivou veze (engl. *link level enforced security*)

Sigurnost na fizičkom sloju

- Četiri entiteta:
  - javne adrese uređaja BD_ADDR (48 bitova)
  - tajnog ključa za proveru identiteta (128 bitova)
  - tajnog ključa za šifrovanje (8 do 128 bitova)
  - slučajno generisane vrednosti RAND (128 bitova)

Upravljanje ključevima

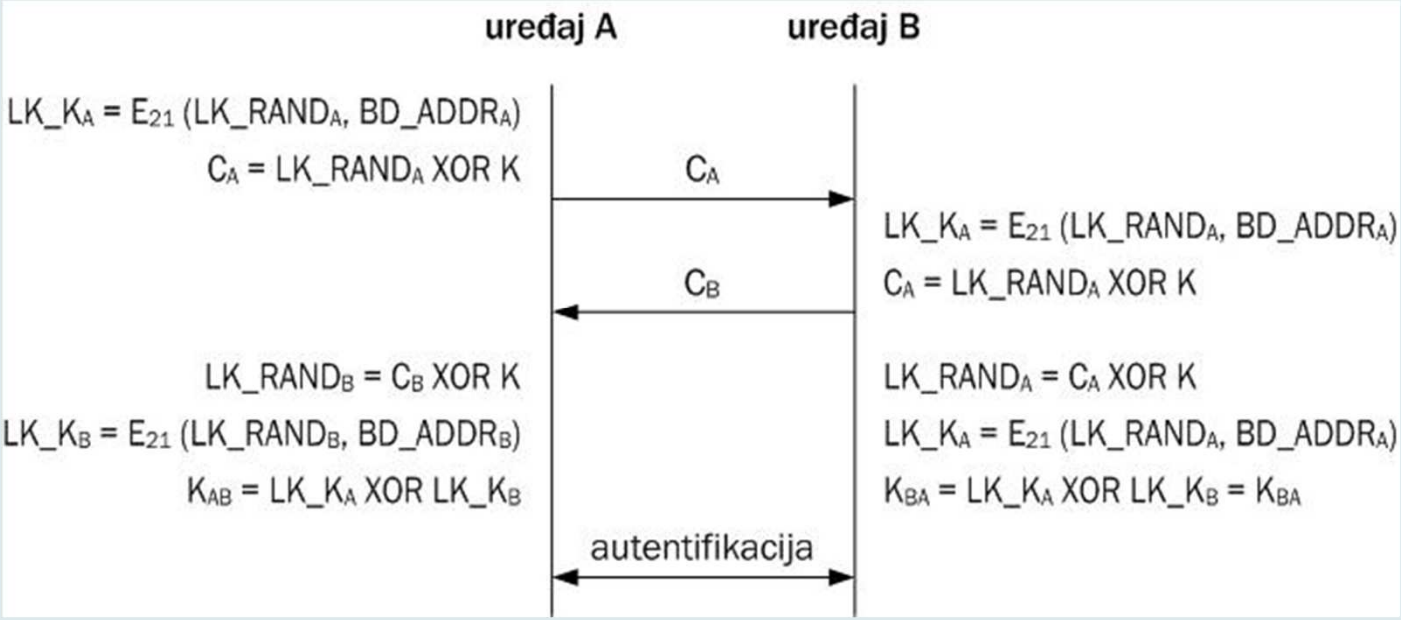
- Definisana su četiri tipa ključa veze kako bi se zadovoljile potrebe različitih vrsta aplikacija:
  - inicijalizacioni ključ K_{init} (engl. *initialization key*)
  - jedinični ključ K_A (engl. *unit key*)
  - kombinacioni ključ K_{AB} (engl. *combination key*)
  - privremeni glavni ključ K_{master} (engl. *temporary key*)

Generisanje ključeva

- Procedura inicijalizacije se sastoji iz sledećih koraka:
  - generisanje inicijalizacionog ključa,
  - provera identiteta,
  - generisanje ključa veze,
  - razmena ključa veze,
  - generisanje ključa za šifrovanje u svakoj jedinici.

- Nakon procedure inicijalizacije započinje komunikacija ili se veza prekida.

Generisanje kombinacionog ključa



Napadi na Bluetooth

- *Bluejacking*
- *Bluebugging*
- *Bluesnarfing*
- Napad odbijanjem usluge (engl. *Denial of Service*, DoS)
- Uparivanje na javnom mestu može biti riskantno u pogledu sigurnosti?

- Car *whisperer*
- Crv Cabir

Ostali sigurnosni problemi

- Više u o ovoj temi knjizi “Sigurnost računarskih sistema i mreža”
- Seminarski radovi

Literatura

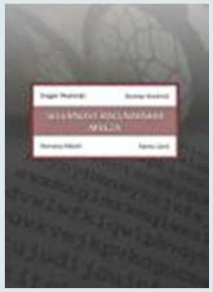
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

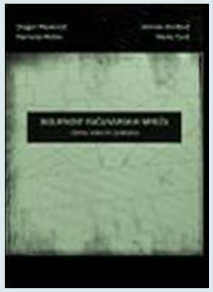
- Za predavanje 9:
  - Poglavlje 9: Sigurnost bežičnih i mobilnih mreža

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?