TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Nastavni predmet:	**UVOD U RAČUNALNE MREŽE**
Vježba:	LV28: Što je sigurnosni ključ mreže i gdje se nalazi (kod usmjernika, Windows sustava i Android mobilnih uređaja)
Cilj vježbe:	Definirati i objasniti ideju i tipove sigurnosnog mrežnog ključa, upoznati se sa primjenama tog ključa u slučaju raznih mrežnih uređaja i okolina (PC, usmjernik, Android telefon)

PRIPREMA ZA VJEŽBU

1. Što u mrežnoj komunikaciji označavaju pojmovi autentifikacija i autorizacija?
2. Što u mrežnoj komunikaciji označava pojam vjerodajnica?
3. Što se podrazumijeva pod pojmom host?
4. Što u računalstvu označav pojam hakiranje? Što znači etičko hakiranje?

IZVOĐENJE VJEŽBE

Što je sigurnosni ključ mreže (Network Security Key)?

Tzv. **network security key** predstavlja vrstu mrežne lozinke (*password, passphrase*) u obliku fizičkog, odnosno digitalnog potpisa ili lozinke biometrijskih podataka koji se koriste s ciljem osiguravanja autorizacije i pristupa bežičnoj mreži ili uređaju sa kojim se klijent ili korisnik želi povezati.

Sigurnosni ključ također omogućuje ostvarivanje sigurne veze između klijenta (koji zahtjeva) i mreže ili bežičnog uređaja, npr. usmjernika (koji poslužuje). Na ovaj se način štiti mrežu i uređaje od neželjenog pristupa.

Različite su vrste sigurnosnih ključeva, a koriste se na raznim mjestima prilikom svakodnevnih usluga kao što su *online banking* i novčane transakcije u obliku OTP-a (*one time password*), *online shopping*, pristup internetskim servisima, pristup (*login*) na elektroničku poštu (*mail account*) ili neki mrežni uređaj i dr.

Vrste sigurnosnih ključeva mreže

Najčešće vrste sigurnosnih ključeva koje se koriste prilikom autorizacije na bežične mreže uključuju *Wi-Fi protected access* (WPA and WPA2) ili *wired equivalent privacy* (WEP) način.

1. WEP

WEP koristi 40-bitni ključ za enkripciju podatkovnog paketa. Taj je ključ kombiniran sa 24-bitnim IV (inicijalizacijskim vektorom) kako bi se stvorio tzv. RC4 ključ. Tih 40 bita i 24 bita od IV zajedno čine 64-bitni WEP ključ. Pri tom se koriste dvije vrste autentifikacijskih metoda: *open system* i *shared key* autentifikacija.

U *open system* autentifikacijskoj metodi, *host* klijenta koji zahtjeva vezu ne treba prezentirati vjerodajnice pristupnoj točki kako bi se autentificirao. U procesu enkripcije koristi se samo WEP ključ.

Prilikom *shared key* autentifikacije, WEP ključ se koristi za autentifikaciju primjenom procesa četverostrukog *challenge-response* rukovanja.

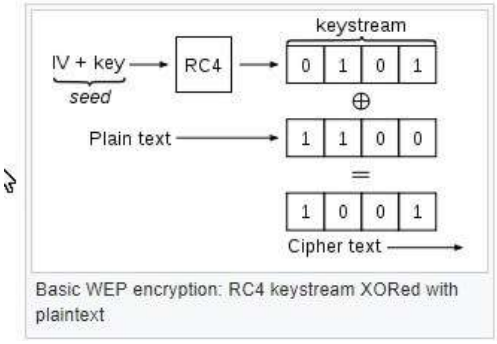
Pri tom, prvo *host* (klijent) šalje autentifikacijski zahtjev pristupnoj točki. Nakon toga, pristupna točka u odgovoru vraća tzv. *clear-text challenge*. Upotrebom WEP ključa, host (klijet) enkriptira tekst izazova i šalje ga natrag pristupnoj točki.

Nakon toga, pristupna točka dekriptira odgovor i ako je on identičan tekstu izazova, prenijet će pozitivan *reply*, nakon čega se kompletira process autentifikacije i pridruživanja, a WEP ključ (pomoću RC4) koristi za enkripciju podatkovnih paketa.

Iako naizgled siguran proces, ključ može biti jednostavno dekodiran razbijanjem okvira izazova. Zbog toga je ova metoda enkripcije i autentifikacije manje u upotrebi i razvijen je mnogo sigurniji WPA.)

ZADATAK: Odaberite proizvoljni alat koji se može koristiti kod bežičnog hakiranja i ukratko ga opišite. Ako ste u mogućnosti, instalirajte i pokušajte raditi sa tim alatom. Komentirajte svoje iskustvo.

Prikaz WEP enkripcije



Basic WEP encryption: RC4 keystream XORed with plaintext

#2) WPA i WPA2

Host uređaj koji se želi spojiti na mrežu zahtjeva sigurnosni ključ kako bi započeo komunikaciju. WPA i WPA-2 rade na principu da se nakon validacije ključa, razmjena podataka između *host* uređaja i pristupne točke obavlja u enkriptiranom obliku.

WPA isporučuje *temporal key integrity protocol* (TKIP) koji koristi tzv. *per- packet* ključ što znači da dinamički proizvodi svježi 128-bitni ključ svaki put kad paket stigne. Ovo paket čuva od neželjenih pristupa i napada.

Ovaj process ima tzv. *message integrity check*, koji čuva podatke od virusa koji bi mogli promijeniti i ponovno slati izmijenjene pakete, te tako mijenja *cyclic redundancy check* (CRC) metodu za detekciju pogrešaka i ispravke koju koristi WEP.

Ovisno o vrsti korisnika WPA dijelimo na:

WPA i WPA-2 -Personal (WPA-PSK): Koristi se za kućne mreže i male uredske mreže jer ne treba poslužiteljski baziranu autentifikaciju. Podaci su enkriptirani na osnovu izlučivanja 128 bitnog ključa iz tzv. *pre-shared* ključa od 256 bita.

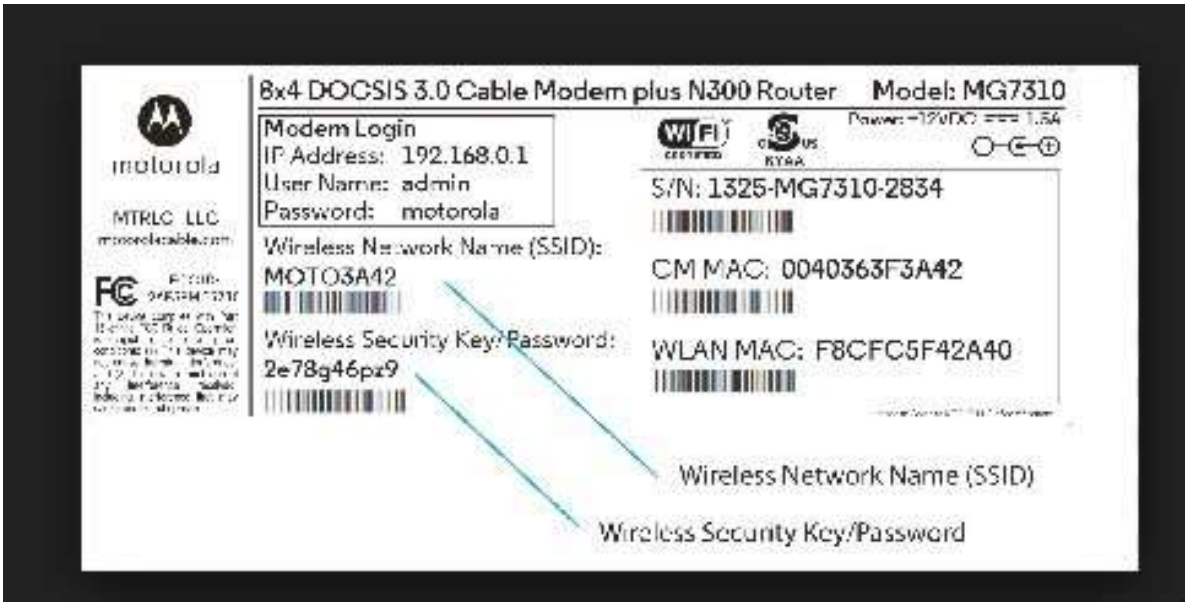
WPA i WPA2 Enterprise: Isporučuje 802.1x i RADIUS server poslužiteljsku autentifikaciju koja je mnogo sigurnija, a uglavnom se koristi prilikom procesa autorizacije i autentifikacije u poslovnim organizacijama.

Kako i gdje pronaći sigurnosni mrežni ključ na usmjerniku?

Sigurnosni ključ mreže igra vrlo važnu ulogu kod povezivanja uređaja na usmjernik kako bi pristupili Internetu. Ako je netko promijenio sigurnosni mrežni ključ ili se on zaboravi, pristup uslugama Interneta bit će onemogućen.

Sigurnosni mrežni ključ usmjernika označen je na uređaju kao "*security key*", "*WEP key*"," *WPA key*" or "*passphrase*". Također, može se pronaći i u priručniku koji dolazi sa kupljenim usmjernikom.

O sigurnosnom mrežnom ključu usmjernika može se naučiti i prijavljivanjem na njegove podrazumijevane postavke na mrežnom sučelju tog usmjernika.



ZADATAK: Ako imate dostupan bežični usmjernik, pokušajte sami naći njegov sigurnosni ključ.

TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Kako pronaći sigurnosni ključ mreže za Windows10?

Sigurnosni mrežni ključ za Windows PC ili laptop je WI-Fi lozinka za spajanje na Internet.

Koraci za upisivanje:

- start menu -> odaberite settings -> odaberite network and Internet -> Network and sharing center.
- Odaberite ime mreže sa kojom se želite spojiti -> Wi-Fi status -> wireless network properties.
- Odaberite network security key -> unesite lozinku i pritisnite tipku next. Nakon provjere mrežnih zahtjeva i nakon dohvaćanja IP adrese, izvršava se spajanje na internet.

Ako je PC spojen na mrežu, upamtit će lozinku ili sigurnosni ključ mreže na koju je spojen, ali ako je potrebno naći lozinku može se slijediti korake:

1. control panel -> odabrati **network and internet**.
2. Odabrati manage wireless networks -> kliknuti network SSID na koji je spojen.
3. Desni klik na ime mreže i klik na properties -> odabrati *security* tab.
4. **Označiti show characters.**

ZADATAK: Ako imate računalo spojeno na bežičnu mrežu, izvedite i provjerite ove korake.

Kako pronaći sigurnosni mrežni ključ za **Android?**

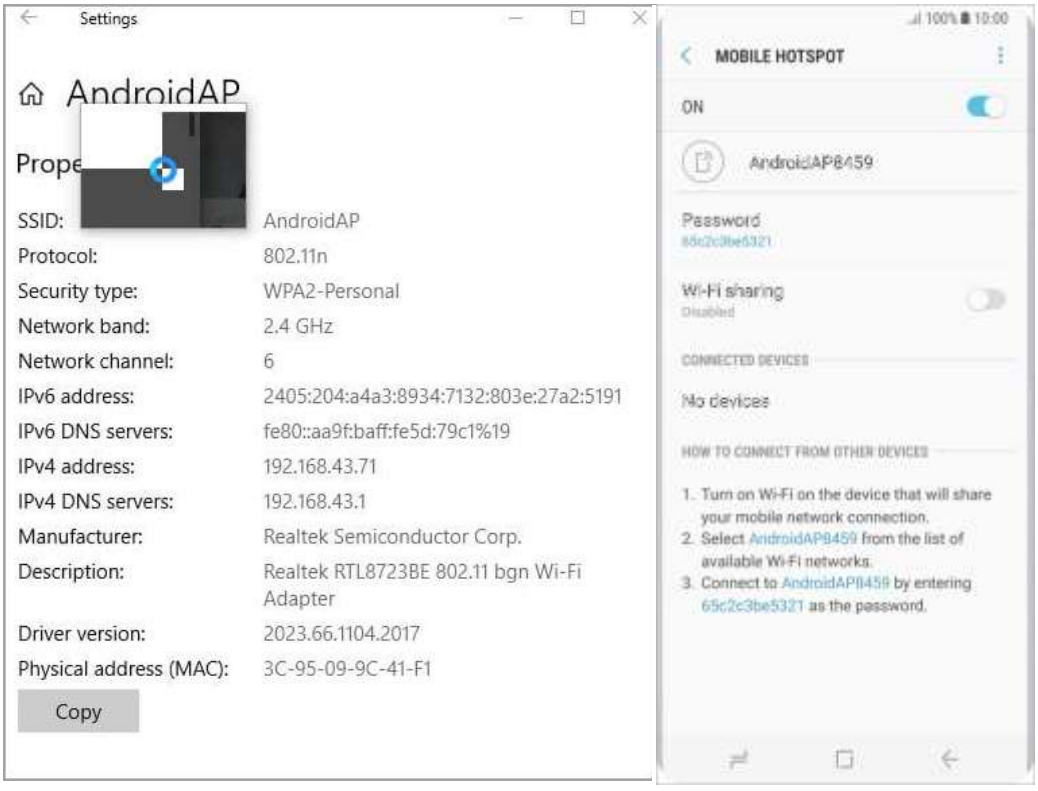
3G i 4G označavaju LTE mobilne android uređaje sa podrškom upotrebe podataka odnosno pristupa Internetu na samom uređaju. Potrebno je samo omogućiti *mobile data* na android uređaju kako bi se takve podatkovne usluge aktiviralo.

Međutim, za uparivanje android uređaja sa drugim uređajima koji će se tako isto moći spojiti na Internet, potreban je mrežni sigurnosni ključ kako bi se napravio tzv. *mobile hotspot*.

Suvremeni pametni telefoni u postavkama imaju ikonu kojom se omogućuje *mobile hotspot*, te mi preko toga možemo dopustiti uparivanje uređaja sa android mobilnim telefonom (*mobile hotspot* radit će samo ako je istovremeno omogućeno *mobile data*).

Koraci za omogućavanje *mobile hotspot* i unosa sigurnosnog mrežnog ključa:

- wireless and networks settings na android telefonu -> *tethering and portable hotspot* option.
- WLAN ili Wi-Fi hotspot -> omogućiti *WLAN hotspot mode*.
- Odabrati set up a WLAN hotspot option -> ispisuje se *default network SSID* (ime mreže vašeg android telefona), tip sigurnosti (open, WPA-PSK ili WPA2-PSK) i sigurnosni ključ mreže (*password*). *network SSID* i *password* podrazumijevano su jedinstveni za svaki Android telefon. Na taj se način može pronaći sigurnosni mrežni ključ za android telefon.
- Moguće je mijenjati pojedine postavke po želji i snimiti promjene.
- Uređaj koji želite upariti može pristupiti Internetu nakon unosa mrežnog SSID-a I lozinke u njegovim *wireless and network* postavkama. Time je uspostavljen i aktiviran *hotspot* između telefona i mrežnog uređaja.
- mobile hotspot će funkcionirati dok se usluga ne deaktivira na strani android telefona ili dok se ne prekorači podatkovni limit na android uređaju.
- Ukoliko bi neautorizirani korisnik pokušao pristupiti tom Internetu, moguće ga je blokirati kroz *hotspot* postavke, s obzirom da je na telefonu moguće vidjeti koliko se korisnika spojilo putem telefona.



TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Što je *Network Security Key Mismatch Error* i kako se popravlja

Prilikom spajanja na bežičnu mrežu naših uređaja kao štu su usmjernik, PC, laptop ili Android telefon kako bismo pristupili Internetu u bilo kojoj LAN ili kućnoj mreži, potreban nam je *network security key* kao lozinka za pristup mreži.

Network security key je jedinstvena kombinacija alfanumeričkih znakova i razlikuje se za svaku u tom području dostupnu mrežu. Ako se nakon unosa lozinke pojavi poruka za *network security key mismatch*, to znači da je unijeta kombinacija znakova za pristup mreži neispravna i ne podudara se sa lozinkom te mreže.

Više je načina za ispravljanje te greške koje se može primijeniti kako bi se došlo do ispravnog sigurnosnog mrežnog ključa.

Neki savjeti:

- Najčešći razlog ove greške je unos krive lozinke (npr. velika/mala slova)
- Ako je unijeta lozinka ispravna, a greška se ipak javlja, može se pokušati ponovno pokrenuti uređaj (usmjernik ili PC).
- Jedan od uzroka pogreške može biti da Wi-Fi mreža kojoj pokušavate pristupiti nije kompatibilna sa uređajem. U tom slučaju provjerite koju inačicu Hence, Wi-Fi mreže može podržati vaš uređaj i nakon toga se pokušajte prijaviti samo u neku od tih mreža.
- Ako ne pomaže ništa od navedenog, primjenjuje se resetiranje čitavog sustava. Prijavite se na usmjernik i kreirajte novo ime za mrežu i novi sigurnosni ključ i zabilježite ga ispravno radi pamćenja.
- Nakon toga u PC ili laptop *network and sharing center* postavkama obrišite sve detalje mreže i ponovno pokrenite PC.
- Ponovno potražite mrežu na koju se želite spojiti i zatim dodajte novi *network security key*.

ZADATAK: Opišite ukratko neko svoje iskustvo i postupak koji ste primijenili prilikom rješavanja problema kod spajanja na bežičnu mrežu.

TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Je li Network Security Key isto što i lozinka?

Sigurnosni ključ je tehnički pojam koji se općenito koristi kod usmjernika, preklopnika i modema, kod kojih postoji za svaki mrežni SSID jedinstveni i različit tip sigurnosnog ključa koji se naziva *WPA* key ili *WPA2 key* ili *passphrase* ovisno o proizvođaču mrežnog uređaja.

Također za windows PC, *network security key* kao lozinka se koristi zajedno sa imenom mreže kako bi se pristupilo bežičnoj mreži. Ključ je samo jedinstvena kombinacija alfanumeričkih znakova.

Općenito, prilikom pristupa internetskim servisima sa android telefona, sigurnosni ključ bit će ispisan kao lozinka za aktivaciju servisa. Prema tome, isto je samo se koriste različite terminologije ovisno o proizvođaču uređaja, vrsti uređaja i mrežnoj okolini.

Za sve zadatke bilješke napravite u bilježnici ili na vlastitom mrežnom sjedištu.