Sigurnost bežičnih (WIFI) mreža

Sadržaj

- Protokol 802.11
- Preporuke za kućne korisnike
- Rizici
- Podešavanje sigurnosnih postavki
- Korištenje otvorenih mreža
- Rješenja za autentifikaciju korisnika

Karakteristike

- Spajanje mobilnih uređaja i računala na Internet
- Povezanost bez obzira na vrijeme ili lokaciju
- Za komunikaciju putem zraka (radiovalovima) koriste protokol IEEE 802.11
- Ozbiljni sigurnosni rizici (odavanje povjerljivih podataka)
- Presretanje i špijunaža internetskog prometa korisnika

Karakteristike (2)

- Valovi koji prenose podatke šire se u svim smjerovima i svatko tko je u dometu može se pokušati spojiti na mrežu te izvršiti zlonamjerne radnje
- Rješenja: podešavanje usmjernika prema sigurnosnim standardima kako bi onemogućili zlonamjerne korisnike u pokušaju ugrožavanja sigurnosti ostalih spajanjem na istu infrastrukturu

Protokol 802.11

- Omogućuje standardizaciju, jednako korištenje korisnicima i proizvođačima opreme
- IEEE grupa protokola s ciljem implementacije i razvoja bežične lokalne komunikacije (WLAN)
- Inačice se razlikuju prema: brzinama prijenosa, frekvenciji na kojoj rade, udaljenostima na kojima je moguć prijenos podataka, tehnologijama
- Nove inačice omogućuju veće brzine prijenosa i kompatibilnost sa prethodnima (neke inačice 802.11n, 802.11ac...)
- 2.4GHz donosi veću pokrivenost signalom, 5GHz nudi veće brzine prijenosa

Rizici

- Kad se osoba spoji na mrežu koja je pod vašom adiministracijom, **vi ste odgovorni za sve** (potencijalno) nezakonite radnje koje napravi
- Izvršavanje napada na druge računalne sustave, preuzimanje materijala pod autorskim pravima (intelektualno vlasništvo) ili nekog sadržaja koji upućuje na neku kriminalnu djelatnost

Rizici (2)

- Kad se napadač (zlonamjerni korisnik, cracker) nalazi u određenoj mreži, pomoću različitih programa za prisluškivanje podatkovnog prometa može doznati privatne podatke o vama, vašim navikama na internetu (mrežne stranice koje posjećujete, lozinke koje koristite i dr.), može podići svoju bežičnu mrežu s istim nazivom (SSID – service set ID) poput neke legitimne s namjerom da prisluškuje promet i tako pokuša doći do vrijednih korisničkih podataka (evil twin napad) (pomaže mu to što kartice računala i mobilnih uređaja češće odabiru spajanje na mrežu (SSID) koja ima jači signal)

Podešavanje sigurnosnih postavki

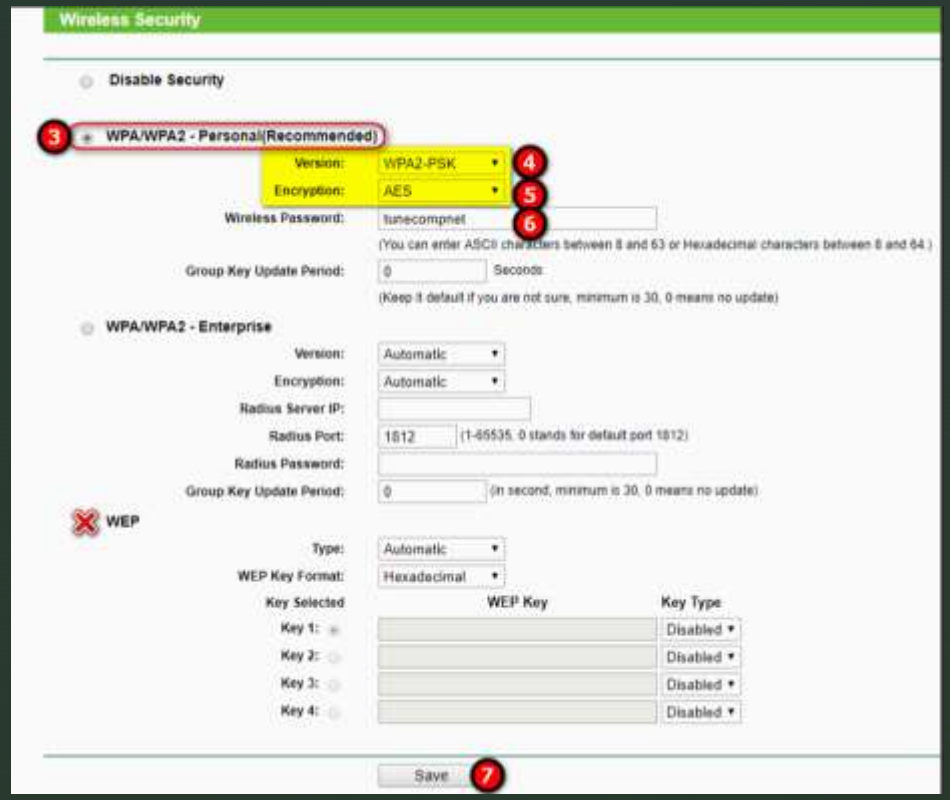
- 1. promjena inicijalne lozinke za prisup postavkama usmjernika
- Objašnjenje: svatko u mreži može se pokušati spojiti na administratorsko sučelje usmjernika te mijenjati sigurnosne postavke
- Upute za konfiguriranje, inicijalne lozinke za pristup konfiguraciji nalaze se na mrežnim stranicama pružatelja Internet pristupa
- Napadač ispitivanjem malog broja lozinki može doći do pristupa usmjerniku u slučaju da vlasnik mreže nije promijenio inicijalnu lozinku

Podešavanje sigurnosnih postavki (2)

- 2. postavljanje lozinke i odabir sigurne metode šifriranja podataka koji se prenose
- Izbjegavati postavljanje kratke i jednostavne lozinke poput imena vezanih uz obitelj, kratki niz brojeva i sl.
- Objašnjenje: napadač teže pogađa lozinku alatima koji koriste veliki broj pokušaja i pogrešaka (brute force)
- Minimalna preporučena dužina lozinke je kombinacija 15 nasumično odabranih brojeva, slova i znakova

Šifriranje komunikacije između računala i usmjernika

- Najrašireniji protokoli su WEP i WPA/WPA2



WEP – Wired Equivalent Privacy

- Najstariji protokol za šifriranje bežičnih mreža
- Manje se koristi jer su otkriveni sigurnosni propusti u protokolu zbog kojih je moguće u roku od nekoliko minuta doći do ključa potrebnog za dešifriranje, odnosno spajanje na mrežu

WPA/WPA2

- Wi-Fi Protected Access
- Prilikom postavljanja metode šifriranja moguće je odabrati između više različitih verzija protokola (WPA-TKIP, WPA-AES, WPA2 Enterprise i dr.)
- Preporuka je korištenje WPA2 protokola uz AES metodu šifriranja (WPA2 Personal). Enterprise verzija koristi dodatni server za autentifikaciju korisnika i pogodna je za poslovne korisnike radi skalabilnosti i lakšeg administriranja
- Uz dovoljno dugu lozinku vrlo je teško dešifrirati bežičnu komunikaciju prilikom korištenja WPA2-AES protokola

WPS (WiFi Protected Setup)

- Za jednostavnije spajanje bežičnih uređaja bez dodatnih konfiguracija i znanja lozinke
- Implementacije: u obliku PIN-a od osam znamenki koji se obično nalazi na poleđini usmjernika. PIN se upisuje u prijenosni uređaj koji se želi spojiti na mrežu, nakon čega usmjernik automatski šalje uređaju sve postavke (uključujući i lozinku za šifriranje podataka), no metodom pokušaja pogađanja PIN-a moguće je u kraćem vremenskom intervalu doći do lozinke. Drugi način je WPS tipka na usmjerniku ili u postavkama, no i to predstavlja značajan sigurnosni problem. Preporuka je onemogućiti.

O postavkama sigurnosti

1. WEP šifriranje nije dovoljno sigurno za korištenje
2. Ograničavanje oglašavanja SSID-a (identifikatora bežične mreže) nije dovoljno jer ga napadač uz odgovarajuće alate može otkriti
3. Filtriranje MAC adresa nije sigurno jer postoje alati koji mijenjaju MAC adresu, pa napadač jednostavno postavi MAC adresu svog računala da bude jednaka nekoj adresi računala koje ima dopuštenje spajanja na mrežu
4. Limitiranje ili isključivanje DHCP poslužitelja nije dovoljno jer napadač može doznati adresu mreže i statički konfigurirati IP adresu iz odgovarajućeg raspona
5. Limitiranje jačine signala kako bi se smanjila pokrivenost nije zaštita jer se može nabaviti mrežne kartice sa snažnim antenama koje hvataju signal i na udaljenostima većim od jednog kilometra

Redovite nadogradnje firmwarea

- Važno je instalirati nove inačice ugrađenog softvera za usmjernik sukladno njihovim objavljivanjima
- Proizvođač radi i izdaje zakrpe za otkrivene probleme
- U slučaju zastarjele inačice firmwarea, napadač iskorištava poznatu ranjivost kako bi pristupio mreži, odnosno računalima u njoj

Za korisnike otvorenih (javnih) mreža

- Zlonamjerni korisnici mogu se pozicionirati između korisnika i pristupne točke te tako dobiti pristup osjetljivim podacima (mailovima, kreditnoj kartici, lozinkama za spajanje na portale i sl.)

Poboljšanje sigurnosti kod korištenja otvorenih mreža (1)

- Korištenje VPN-a (Virtual Private Network) – VPN šifrira sav internetski promet između korisnika i mrežnog servera pružatelja VPN usluge. Pružatelj usluge je posrednik koji prosljeđuje promet na odredišne lokacije i vraća šifrirane odgovore korisniku. Zlonamjerni haker svojim pozicioniranjem između korisnika i njegove pristupne točke dobija samo uvid u šifrirani promet koji je za njega nečitljiv.

Poboljšanje sigurnosti kod korištenja otvorenih mreža (2)

- Korištenje SSL (Secure Sockets Layer) konekcija – SSL je protokol namijenjen sigurnom prijenosu privatnih podataka na internetu korištenjem šifriranja. Mrežna stranica koja koristi SSL protokol za šifriranje podataka između nje i preglednika započinje sa https

Poboljšanje sigurnosti kod korištenja otvorenih mreža (3)

- Isključivanje dijeljenja podataka, odnosno ne dijeliti datoteke sa ostalim korisnicima u mreži

Poboljšanje sigurnosti kod korištenja otvorenih mreža (4)

- Isključivanje bežične kartice kad se ne koristi – mrežna kartica se spaja na pristupnu točku koja emitira jači signal, a automatski se spaja i na mrežu na koju je nekad bila spojena (prema SSID-u). Podizanjem vlastite bežične mreže poznatog imena, haker inicira spajanje bežične kartice nekog uređaja na nju.

Rizici za vlasnike otvorenih mreža

- Vlasnik otvorene mreže je jedina kontakt i odgovorna osoba za sve potencijalne nezakonite radnje koje se odvijaju u njegovoj mreži
- Posljedica je nužnost uvođenja autentifikacije krajnjih korisnika prije nego im se dopusti korištenje mreže.
- Pohranjivanjem podataka o korisnicima (uređaj kojim se spaja, broj mobilnog uređaja, mail adresa...) te pohranjivanjem vremena njihovog spajanja na mrežu, uvodi se mogućnost praćenja korisnika i prebacivanje odgovornosti za zlonamjerna djela na njih.

Uvjeti korištenja

- Prije dopuštanja korištenja bežične mreže (hotela, restorana, zračne luke...) preporučuje se upozoriti korisnika na prihvatljivo korištenje. Korisnike treba upoznati sa pravilima i rizicima korištenja takve mreže
- Implementacija: korisnik se usmjeri na početnu mrežnu stranicu sa uvjetima korištenja:
- Vrsta usluge (osnovni tehnički parametri), mogućnost blokiranja pristupa (u slučaju kršenja pravila), nezajamčena sigurnost, odnosno privatnost, ograničavanje od odgovornosti vlasnika mreže za potencijalnu štetu koju je korisnik pretrpio, zabrana korištenja mreže za zlonamjerne radnje (širenje spama, DDoS, kršenje autorskih prava i dr.)

Rješenja za autentifikaciju korisnika - SMS

- Autentifikacija korisnika na temelju nečeg što posjeduje (mobilni uređaj sa SIM karticom)
- U slučaju SIM kartice korisnik unosi broj svog mobilnog uređaja na kojeg se potom šalje SMS poruka sa PIN-om
- Korisnik unosi PIN u mrežno sučelje
- Na strani pružatelja usluge nalazi se server/baza podataka koja uparuje PIN sa telefonskim brojem
- Kod prvog upisivanja PIN-a u mrežni obrazac pamti se MAC adresa uređaja i uparuje s PIN-om
- Kod ponovnog spajanja provjerava se postoji li asocijacija PIN-a i MAC adrese, ako je nema, pojavljuje se početna stranica za autentifikaciju
- Naprednija izvedba ovog rješenja uključuje bilježenje aktivnosti korisnika u bazu podataka radi kasnije eventualno potrebne forenzike

Rješenja za autentifikaciju korisnika – Agregacija autentifikacija

- Google Identity Toolkit
- Višestruke opcije autentifikacije korisnika pomoću servisa: Google, Facebook, Yahoo, Microsoft, PayPal...
- Prednost je što objedinjuje velike servise sa velikim brojem korisnika
- Zahtjevnije za implementaciju jer je potrebno uvođenje posredničkog servera na kojem se održavaju informacije o autentificiranim klijentima i njihovim pristupnim podacima

Rješenja za autentifikaciju korisnika - Radius

- Radius server je pogodan za velika poslovna okruženja sa velikim brojem korisnika
- Prednost je što na centralnom mjestu sprema informacije o korisnicima i istovremeno omogućuje laku administraciju
- Podaci o korisnicima mogu biti spremljeni u sklopu samog RADIUS servera ili u već postojećoj bazi podataka (LDAP – Lightweight Access Directory Protocol)
- RADIUS server služi kao posrednik koji prima zahtjeve klijenata i upravlja njihovim pristupom resursima

Autentifikacija u hotelima

- Povezivanje prezimena gosta i broja sobe
- Prilikom prijavljivanja gosta podaci o klijentu šalju se u središnju bazu podataka
- Sav internetski promet koji dolazi od neautentificiranog uređaja se presreće te preusmjerava na captive portal u kojem gost mora unijeti tražene podatke
- Ako se podaci podudaraju sa podacima u bazi, gostu se omogućuje pristup internetu
- Prilikom odjavljivanja gosta, briše se asocijacija i tako se održava sigurnost