Bezbjednost i zaštita informacionih sistema

4. Sigurnost bežičnih mreža (WLAN)

Bežične tehnologije

Budući da u današnje vrijeme postoji veliki broj bežičnih tehnologija koje se mogu primjenjivati u različitim oblastima u ovom dijelu će se izvršiti klasifikacija tih tehnologija po njihovom dometu. **U klasifikaciji po dometu, bežične tehnologije možemo svrstati u**:

- **WWAN (Wireless Wide Area Network)**
- **WMAN (Wireless Metropoliten Area Network)**
- **WLAN (Wireless Local Area Network)**
- **WPAN (Wireless Personal Area Network)**

Bežične tehnologije

Wireless Wide Area Networks (WWAN) su mreže širokog područja, kao i WAN (Wide Area Network) mreže, samo što koriste bežične tehnologije. Dometa su preko 50 km i u ovakvim sistemima za povezivanje se koriste tehnologija mobilne telefonije kao što su LTE i UMTS.

Wireless Metropolitan Area Networks (WMAN) su mreže gradskog područja. Dometa su u rasponu do 50 km. Pored tehnologija mobilne telefonije, u ovim okruženjima najpopularnija tehnologija je WiMAX.

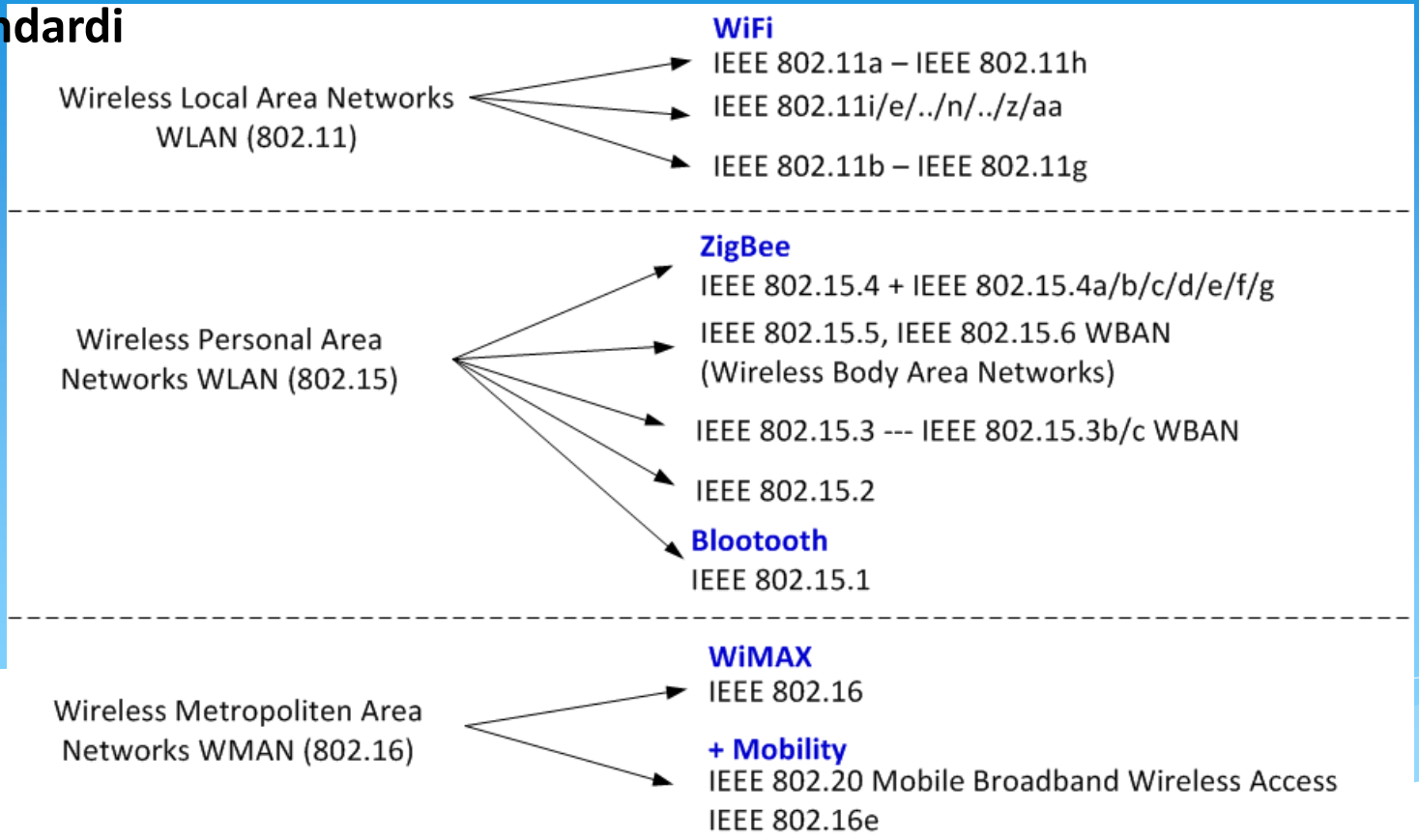
Wireless Local Area Networks (WLAN) su lokalne mreže. Dometa su do 100 m. U ovim okruženjima se najviše koriste WLAN tehnologije ili IEEE 802.11 serija standarda.

Personal area network (PAN) ili mreže personalnog područja su računarske mreže koje služe za prenos padataka između uređaja kao što su računari, telefoni, periferni uređaji i personalni digitalni uređaji i sl. PAN mreže se mogu koristi za međusobno povezivanje uređaja ili za povezivanje na mreže višeg nivoa ili Internet. PAN može da koristi žičane medije za povezivanje kao što su USB i FireWire.

Wireless Personal Area Network (WPAN) je bežična PAN mreže koja može da koristi jednu od sljedećih tehnologija:

- Bluetooth i Bluetooth Low Energy (BLE)
- ZigBee
- Z-Wave
- 6LoWPAN
- Ultra-Wideband (UWB)
- Body Area Network (BAN)
- IrDA, Wireless USB ...

IEEE 802 standardi



Uvod

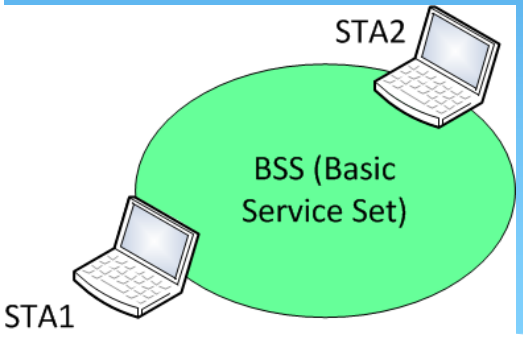
WLAN je skraćenica za engleski naziv **Wireless Local Area Network** i označava lokalnu mrežu **(LAN)** koja se zasniva na bežičnim tehnologijama.

- Prenos podataka bežičnom vezom radio talasima postao je veoma atraktivno rješenje u skoro svim segmentima telekomunikacije,
- U opštem slučaju najbitniji zahtjevi u WLAN-u su visok protok podataka, fleksibilnost, mobilnost korisnika unutar mreže i jednostavnost korišćenja,
- Današnji WLAN-ovi posjeduju svojstva koja ih čine privlačnim za korišćenje sve većeg skupa korisnika.,
- Velikom broju poslovnih korisnika posebno je zanimljiva, a nekima i neophodna pokretljivost u radu. Primjena koncepta pokretljivosti (*mobility*) omogućuje stanicama u WLAN-u permanentno mijenjanje fizičkog položaja uz istovremenu mogućnost međusobnog komuniciranja.

Standardi IEEE 802.11

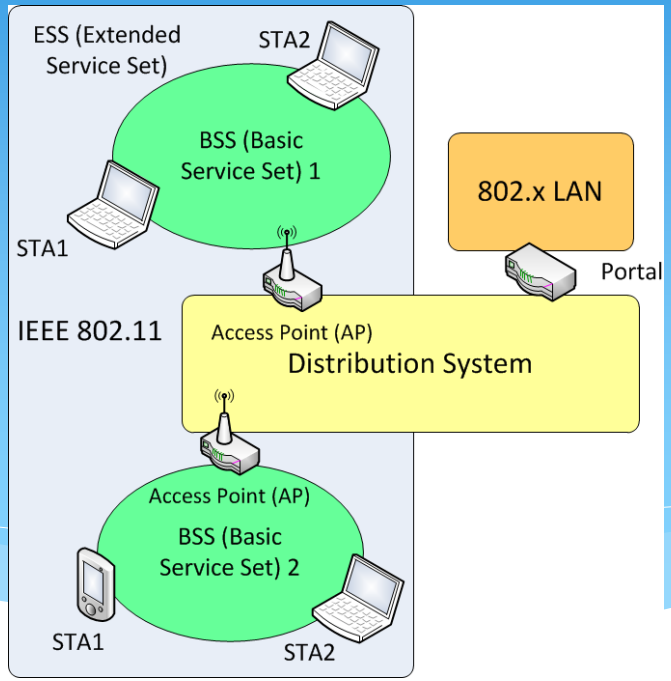
Arhitektura

Sistemska arhitektura kod 802.11 podrazumijeva dvije osnovne arhitekture: infrastrukturno bazirane i ad-hoc.



Arhitektura ad-hoc baziranog 802.11 LAN -a

Arhitektura infrastrukturno baziranog 802.11 LAN -a



Standardi IEEE 802.11

Fizički sloj IEEE 802.11

IEEE 802.11 podržava tri različita medijuma za prenos na fizičkom sloj: jedan sloj se zasniva na **infra-crvenom prenosu (IR)**, a druga dva na radio prenosu, prvenstveno u ISM (Industrial, Scientific, Medical) opsezima od 2.4GHz i 5GHz koji je dostupan svuda u svijetu. **Za prenos se koriste FHSS (Frequency-hopping spread spectrum), DSSS (Direct-sequence spread spectrum) i OFDM (Orthogonal frequency-division multiplexing) tehnike prenosa**.

2.4GHz FHSS 1Mbps 2Mbps	**2.4GHz** DSSS 1Mbps 2Mbps	**5GHz** OFDM 6, 9, 12, 18, 24, 36, 48, 56 Mbps	**2.4GHz** DSSS 5.5, 11 Mbps

Fizički sloj (PHY) za radio prenos kod protokola IEEE 802.11

Standardi IEEE 802.11

Standard 802.11b

Prihvatanje bežičnih mreža na tržištu u velikoj mjeri su usporili relativno mali protoci definisani 802.11 standardnom. Da bi se izašlo u susret potrebama za povećanim protokom **IEEE je 1999. godine odobrio 802.11b**. Standard je zvanično objavljen u oktobru 1999. godine, frekvencija na kojoj radi je 2.4GHz, brzina prenosa podataka iznosi 4.5Mbit/s, **maksimalna brzina prenosa iznosi 11Mbit/s**, udaljenost između radnih stanica u zatvorenom prostoru je približno 35 metara.

Cilj IEEE je bio da ponudi standard koji podržava brzine prenosa podataka kao i 802.3 Ethernet standard. Standard 802.11b podržava pet brzina prenosa podataka: 11Mbit/s, 5.5Mbit/s, 2.1Mbit/s, 1Mbit/s, 512Kbit/s.

Standardi IEEE 802.11

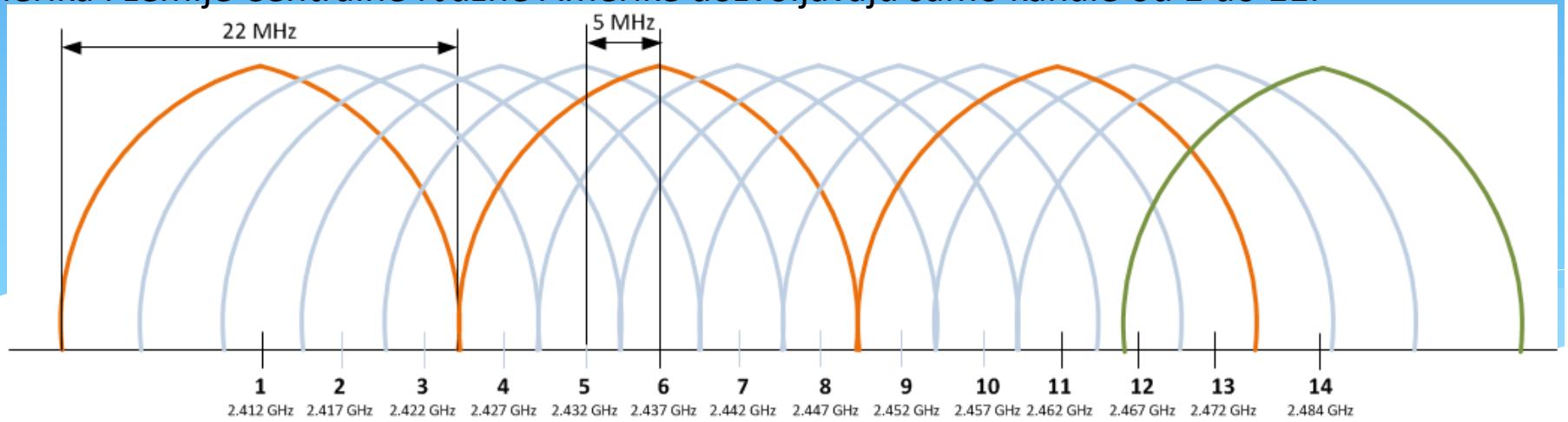
802.11b koristi opseg 2.4GHz u spektru. Riječ je o nelicenciranom radio opsegu poznatom pod imenom – **Industrial, Sceientific and Medical (ISM)** koji u opsegu 2.412-2.483 GHz nudi 14 kanala za korišćenje. Većina WLAN mreža radi na 802.11b standardu pa tako je ovaj standard postao referenca za WLAN.

Varijacija na 802.11b je 802.11b+, koji udvostručuje protok na 22Mbit/s odnosno 44Mbit/s uz Texas instruments ACX100 chipset, pa treba pripaziti prilikom kupovine uređaja.

Zbog toga što 802.11b koristi tehniku proširenog spektra sa direktnom sekvencom (DSSS), svaka 802.11b pristupna tačka može biti postavljena na jedan, ili nekoliko kanala da bi se izbjegao konflikt sa ostalim bežičnim uređajima u okruženju.

Standardi IEEE 802.11

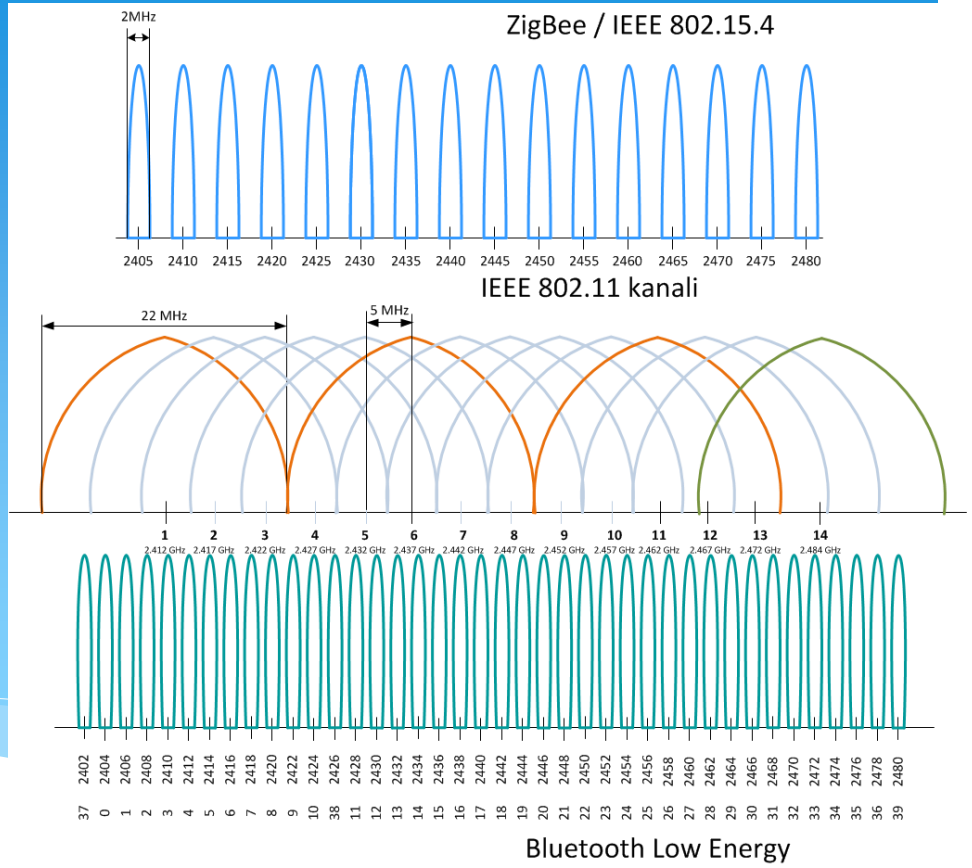
Dostupnost kanala je regulisana različito u različitim državama i regionima, u skladu sa dodjelom radio spektra. Japan dozvoljava upotrebu svih 14 kanala za 802.11b, i 1-13 za 802.11g/n. Španija u samom početku dozvoljava upotrebu jedino kanala 10 i 11, a Francuska jedino kanala 10, 11, 12, i 13. Međutim, sada dozvoljavaju kanale 1 do 13 kao i ostale zemlje Evrope. Sjeverna Amerika i zemlje Centralne i Južne Amerike dozvoljavaju samo kanale od 1 do 11.



Standardi IEEE 802.11

Interferencija (preklapanje pojedinih kanala) kod standarda koji rade u opsegu od 2.4GHz:

- ZigBee i IEEE 802.15.4,
- IEEE 802.11 i
- Bluetooth Low Energy,



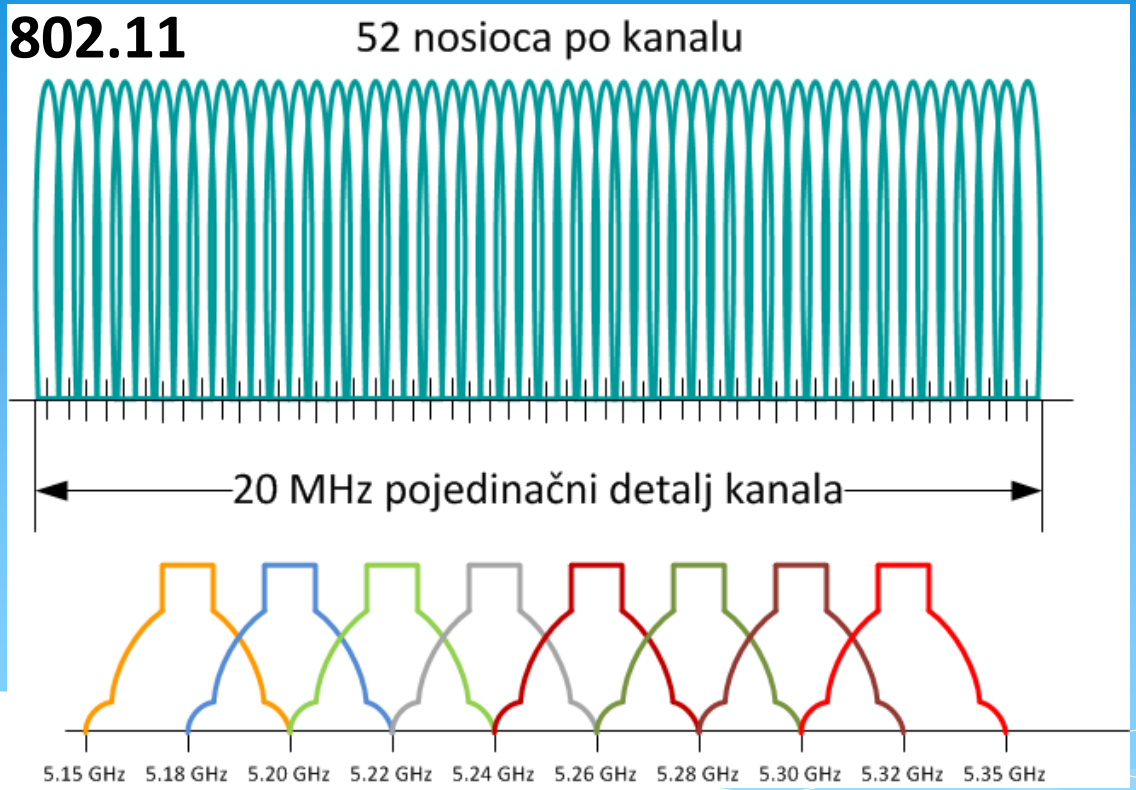
Standardi IEEE 802.11

Standard 802.11a

802.11a je dopunjeni originalni standard rafitikovan 1999. godine. 802.11a standard koristi isti bazni protokol kao i originalni standard, radi u opsegu od **5GHz** i koristi 52 podnosioca (sub carrier) na **ortogonalnim frekvencijama sa multipleksiranjem (OFDM) i maksimalnom brzinom po kanalu od 54Mbit/s, koja daje realnu propusnu moć mreže od 20Mbit/s**.

Kako se došlo do zaključka da opseg na 2.4 GHz nije pogodan za veće brzine prenosa zbog zagušenja, prešlo se na opseg oko 5 GHz, takođe iz ISM dijela spektra. U Evropi je to 5.15 – 5.35 GHz i 5.470 – 5.725 GHz, dok je u SAD to 5.15 – 5.35 GHz i 5.725 – 5.825 GHz.

Standardi IEEE 802.11



Frekvencijski opseg kod 802.11a standarda

Standardi IEEE 802.11

Standard 802.11g

Ovim standardnom predviđen je rad WLAN-a **sa maksimalnim protokom od 54Mbit/s kao kod 802.11a, ali se koriste iste radio frekvencije kao kod 802.11b**, i pri tom je potpuno kompatibilan sa starijom specifikacijom. Kod WLAN mreža koje rade na osnovu standarda 802.11g realna brzina prenosa podataka iznosi **skoro 20Mbit/s** .

U junu 2003. godine IEEE (Institute of Electrical and Electronics Engineers) je zvanično dodao 802.11g protokol u svoju kolekciju sertifikata, a početkom jula proizvođači opreme počeli da objavljuju da su njihovi proizvodi testirani, odnosno sertifikovani u skladu sa zahtjevima, a čime je počela i njihova komercijalna prodaja.

Standardi IEEE 802.11

IEEE 802.11n

Predstavlja jednu od poslednjih izmjena i dopuna koja poboljšava prethodne 802.11 standarde dodavanjem više-predajnih **i više-prijemnih antena po sistemu poznatom pod nazivom MIMO (Multiple Input Multiple Output)**. 802.11n je standard koji predviđa rad uređaja u oba opsega - 2.4GHz i 5GHz.

Brzine prenosa podataka su do 248 Mbps, a propusnost (throughput) 74 Mbps.

IEEE je odobrio izmjene i dopune i to je **objavljeno u oktobru 2009**. Prije konačne ratifikacije, proizvođači su već izvršili migracije na 802.11n mreže bazirane na sertifikatima WiFi alijanse u skladu sa nacrtom standarda 802.11n iz 2007. godine.

Sigurnost bežičnih računarskih mreža

Pitanje sigurnosti je jedno od najčešće postavljanih kada su u pitanju bežične mreže. Pitanje sigurnosti u WLAN mrežama je veoma bitno pitanje s obzirom da se podaci prenose radio talasima.

Zbog načina prenosa postoji mogućnost prisluškivanja i analize saobraćaja što dovodi do otkrivanja povjerljivih informacija, korisničkih lozinki i neautorizovanog pristupa mreži i njenim resursima.

Čak i ako podaci koji se prenose kroz mrežu nisu povjerljivi, postoji mogućnost da uljez koristi nedovoljno zaštićeni WLAN da bi sa njega pokrenuo napade na bilo koji drugi sistem na Internetu.

Sigurnost bežičnih računarskih mreža

Najednostavniji oblik zaštite - Filtriranje MAC adresa

Budući da je MAC adresa jedinstveni heksadecimalni broj svakog proizvedenog mrežnog adaptera, filtriranje daje mogućnost preciznog određivanja uređaja s kojih je moguće pristupiti Access Point-u, odnosno samoj mreži. **Mana ove metode je administriranje statičkih filter lista kod velikih mreža.**

Također, kod nekih mrežnih kartica postoji mogućnost izmjene MAC adrese i predstavljanje pod lažnim brojem. Praktično sve kartice koje imaju podršku za Linux mogu preko sniffer programa sa AP-a pokupiti listu dozvoljenih MAC adresa i zatim ih prikazati kao vlastite. Međutim, kod manjih bežičnih mreža MAC filtriranje je relativno snažan i praktičan oblik zaštite.

Sigurnost bežičnih računarskih mreža

Sigurnost bežičnih pristupnih uređaja ili AP (Access Point) i bežičnih mreža se može klasifikovati u pet kategorija: Open, WEP, WPA, WPA2 i mixed-mode mreže.

Mixed-mode mreže podržavaju WPA i WPA2 isrovremeno. Tih 5 kategorija se kasnije mogu dodatno proširiti podjelom WPA i WPA2 mreža u dvije pod-kategorije kao što su: WPA-Personal i WPA-Enterprise.

Kategorije su određene metodom enkripcije i mehanizmamom za autentifikaciju koji se koriste.

Sigurnost bežičnih računarskih mreža

Generalno, WEP koristi WEP enkripciju, WPA koristi TKIP, a WPA2 koristi CCMP.

Postoji mogućnost da WPA i WPA2 metode koriste i TKIP i CCMP istovremeno zbog pokušaja proizvođača da obezbijede kompatibilnost sa starim uređajima.

Personal WPA i WPA2 koriste PSK (Pre shared key) za lokalnu autentifikaciju, a **Enterprise WPA i WPA2 koriste 802.1x (EAP) i eksterni server za autentifikaciju (RADIUS)**.

Open mreže ne koristi ni šifrovanje ni autentikaciju.

Sigurnost bežičnih računarskih mreža

Wi-Fi Protected Setup (WPS)

WPS je dizajniran od strane Wi-Fi Alliance kako bi se omogućila laka potvrda identiteta uprkos korišćenju složene lozinke. **Ideja je bila da se eliminiše upotreba dugih i složenih lozinki koji nisu prihvatljive za sve korisnike.** Postoji nekoliko varijanti upotrebe WPS. **Iz perspektive bezbjednosti, WPS PIN se smatra nesigurnim.**

Access Point uređaji koji podržavaju ovaj metod imaju taster sa oznakom WPS. Ako se **on pritisne, mora se unijeti WPS PIN na uređaju klijenta u kratkom roku (obično 60 sekundi)**. Ovaj PIN se obično nalazi na naljepnici na AP-a.

Problem sa ovim pristupom je slaba struktura 8-cifarskih PIN-ova, koji se sastoje samo od brojeva. Na taj način, **Brute force napadi se mogu efikasno obavljati u okviru dozvoljenog vremenskog okvira**.

Sigurnost bežičnih računarskih mreža

Wi-Fi Protected Setup (WPS)

Ako ne postoje drugi mehanizmi bezbjednosti za napade na WPS, takvi napadi će biti ponovljeni u roku od nekoliko sati. Pošto se WPS PIN ne mijenja automatski, napad može biti prekinut i nastavljen u neko drugo vrijeme. Za razliku od napada na WPA2, napad mora nužno biti usmjeren protiv Access Point.

Postoji nekoliko besplatnih alata specijalizovanih za ovu vrstu napada, npr. Reaver. Mehanizmi bezbjednosti koji su implementirani u Access Point uređajima mogu blokirati WPS mode u slučaju da postoji suviše PIN-pokušaja u kratkom vremenskom periodu. Reaver može zaobići ove mehanizme i druge mjere zaštite. Ako Reaver alat uspješno obavi posao, Wi-Fi lozinka će se prikazati kao običan tekst.

U većini pristupnih tačaka, WPS je uključen u default režimu, i u PIN modu. Budući da većina korisnika pretpostavlja da je jaka WPA2 lozinka dovoljna za sigurnu mrežu, često zaboravi da isključi WPS, što predstavlja problem za sigurnost uređaja.

Sigurnost bežičnih računarskih mreža

Bežične metode za šifrovanje

Tri metode šifrovanja rade na drugom sloju OSI modela i definisane su 802.11-2007 standardima. **Te tri metode su: WEP, TKIP i CCMP**. One se koriste za šifrovanje MAC protokol Data Unit (MPDU) payload-a, ili podataka sadržanih u IP paketima. Sve tri metode koriste simetrične algoritme. **WEP i TKIP koriste RC4 enkripciju (Stream šifrovanje), dok CCMP koristi AES (Advanced Encription Standard) enkripciju (Block šifrovanje).** IEEE 802.11- 2007 standardi definišu WEP kao metod enkripcije za pre–RSNA security period, dok TKIP i CCMP se smatraju usaglašenim sa Robust Security Network (RSN) protokolima za šifrovanje. **Naredna razlika između WEP, s jedne strane, i TKIP i CCMP s druge strane je da WEP koristi prekonfigurisan statički ključ koji je ranjiv na napade.** Sa druge strane, TKIP i CCMP koriste ključeve za šifrovanje koji se dinamički generišu u okviru 4-way Handshake procesa.

Sigurnost bežičnih računarskih mreža

WEP

Wired Equivalent Privacy (WEP) je najjednostavniji oblik bežične sigurnosti. **To je bezbjednosni protokol drugog sloja koji koristi Rivest Cipher 4 (RC4) streaming šifriranje.** Koristi dvije varijante relativno kratkog dijeljenog ključa: 64-bitnu i 128-binu varijantu.

Standardni 64-bit WEP koristi 40-bitni ključ (takođe poznat kao WEP-40), koji se nadovezuje sa 24-bitnim vektorom inicijalizacije (initialization vector IV) da bi se formirao RC4 ključ. Ovaj metod sigurnosti je samo malo sigurniji vid tekstualne lozinke. Razlog je slabost u WEP protokolu. **WEP zaštita može biti kompromitovana u nekoliko minuta, kad se koriste open-source i široko dostupni alati na Internetu.** Ako se paketi podataka snimaju dovoljno dugo, lozinka se može otkriti u nekoliko minuta. Zbog toga se mreže i pristupne tačke koje koriste WEP smatraju izuzetno nesigurnim.

Sigurnost bežičnih računarskih mreža

WPA

WPA je baziran na IEEE 802.11i standardu. Uveden u aprilu 2003. godine od strane Wi-Fi Alliance organizacije. Upotreba TKIP enkripcije je definisana u standardu sa ciljem prevazilaženja slabosti WEP protokola. **TKIP koristi Rivest Cipher 4 (RC4) streaming šifrovanje za proces enkripcije i dekripcije**. TKIP mijenja WEP sa dužim 128-bitnim per-packet ključem i dinamički generiše 48-bitni vektor inicijalizacije (IV) sa Message Integrity Check (MIC) za svaki novi paket. MIC je dizajniran da bi se spriječili aktivni ili pasivni man-in-the-middle napadi. **Pošto je WPA osmišljen kao privremeno kratkoročno rješenje za poboljšanje bežične sigurnosti, ima i svoje slabosti. WPA treba koristiti samo na starijem hardveru koji nije u stanju da podrži AES-CCMP.** TKIP je obavezan kada se koristi WPA.

Sigurnost bežičnih računarskih mreža

Autentifikacije u bežičnim mrežama

Kao što je opisano na početku WPA i WPA2 imaju podršku za dva metoda autentifikacije: Personal i Enterprise.

Personal metod je lokalna autentifikacija, koja se obično koristi.

Enterprise provjera autentičnosti je zasnovana na upotrebi eksternog servera za autentifikaciju i mnogo manje je prisutna. Zahtijeva poseban server za potvrdu identiteta i namijenjen je prvenstveno za kompanije.

Sigurnost bežičnih računarskih mreža

Personal autentifikacija

Personal WPA i WPA2 mreže su namijenjene da se koriste za ad-hoc konfigurisane pristupe tačke (AP) i kućne mreže. **Oni koriste pre-shared key (PSK) ključ koji je podložan napadima sa pogađanjem password/passphrase s korišćenjem rječnika napada.** PSK podešavanje počinje sa definisanjem passphrase na pristupnoj tački (AP), koja će se koristiti za generisanje ključeva za šifrovanje.

U cilju stvaranja bezbjedne fraze za pristup (passphrase), preporuka je da je ona složena sa više od 20 znakova. **Reijči iz rječnika ne treba da se koriste i passphrase mora da sadrži mala i velika slova, brojeve i specijalne znakove.** Ako se ove preporuke ne slijede, mreže su podložne kompomitovanju.

Sigurnost bežičnih računarskih mreža

Enterprise autentifikacija

Enterprise autentifikacija koristi IEEE 802.1x i eksterni server za autemtifikaciju kao što je Remote Authentication Dial In User Service (RADIUS). Tako ovaj proces definišu tri standarda: EAP, 802.1x, i RADIUS.

The Extensible Authentication Protocol (EAP) je protokol drugog sloja proces koji omogućava bežičnom klijentu autentikaciju na mrežu. Postoji verzija EAP protokola koji se koristi u LAN okruženju i naziva se EAP-over LAN (EAPoL) i verzija za bežične mreže. EAP definiše standardni način enkapsulacije informacija za potvrdu identiteta, kao što su korisničko ime i lozinka ili digitalni sertifikat koje AP može da koristiti za provjeru identiteta korisnika.

Sigurnost bežičnih računarskih mreža

Enterprise autentifikacija

Proces potvrde identiteta se odvija izvan AP-a u komunikaciji sa serverom za provjeru autentičnosti. EAP ima nekoliko proširenja: EAP-MD5, EAP-TLS, LEAP (Lightweight EAP), PEAP (Protected EAP), EAP-Fast i EAP-GTC.

802.1x i RADIUS definišu i pakete za EAP informacije, na primjer 802.1x standard definiše transport od klijenta do pristupne tačke ili uređaja (AP, svič, ruter, itd).

Ovi podaci se prenose pomoću RADIUS protokola za autentifikacione servere. Server će provjeriti autentičnost korisnika i na osnovu toga mu dozvoliti pristup mreži.

Sigurnost bežičnih računarskih mreža

Alati za procjenu sigurnosti bezbjednosti bežičnih mreža

Brojni softverski alati se mogu koristiti za obavljanje wardriving procesa – procesa procene sigurnosti bežičnih mreža. Upotreba alata takođe zavisi od hardverskih i softverskih platformi koje se koriste.

U slučaju korišćenja računara sa **operativnim sistemom Windows** mogući alati su **Vistumbler, InSSIDer, itd**. U slučaju korišćenja **Linux operativnog sistema, Kismet predstavlja de-facto standard**. Uvođenje **Android smart telefon platformi** je uticalo u velikoj mjeri na proširenje mogućih alata za Wardriving. ti alati su: **Wigle Wi-Fi, War-drive, G-Mon, WiFi finder, WiFi tracker** i dr. Za iOS platformu (koja je dostupna za iPhone i iPad) postoje slični softverski alati, npr. WiFiFoFum i Wi-Fi Ekplorer.

Komparacija WEP, WPA i IEEE 802.11i

	IEEE 802.11b WEP	WPA	IEEE 802.11i (WPA2)
Enkripcija	WEP (RC4)	TKIP (RC4)	AES, (opciono TKIP)
Integritet podataka	WEP (RC4) + CRC	TKIP-MIC	AES-MAC (opcionoTKIP-MIC)
Autentifikacija i kontrola pristupa	Autentifikacija sa dijeljenim ključem	IEEE 802.1X/EAP (+ EAP-TLS, LEAP)	IEEE 802.1X/EAP (+ EAP-TLS, LEAP)

Sigurnost bežičnih računarskih mreža

Standard	WEP	802.1x EAP	WPA	802.11i/WPA2
Objavljen	1997	2001	2003	2004
Enkripcija	Statički ključevi, ranjivi	Dinamički ključevi	Dinamički, po paketu	Dinamički, po paketu, najsigurniji
Autentifikacija korisnika	Nema (opciono filtriranje po MAC adresama)	Korisničko ime / lozinka, sertifikati, PSK	Korisničko ime / lozinka, sertifikati, PSK	Korisničko ime / lozinka, sertifikati, PSK

Sigurnost bežičnih računarskih mreža

Mod	WPA	WPA2
Entrprise	802.1x sa EAP autentifikacijom i WEP/TKIP enkripcijom	802.1x sa EAP autentifikacijom i AES enkripcijom
Personal	PSK autentifikacija sa WEP/ TKIP enkripcijom	PSK autentifikacija i AES-CCMP enkripcijom

Zaključak o WLAN sigurnosti

Problem sigurnosti u WiFi mrežama je teži nego u klasičim mrežama. IEEE 802.11 nije riješio sigurnosne probleme na fizičkom i MAC podsloju:

- DoS napadi radio ometanjem (jamming)
- Nepoštovanje procedure za pristup radio kanalu (backoff, NAV, itd.)

WEP protokol

- Nije postigao cilj (ozbiljni sigurnosni problemi

Standard IEEE 802.11i

- Kontrole pristupa je zasnovana na standardu IEEE 802.1X
- Fleksibilan model autentifikacije
- Poboljšano upravljanje kriptografskim ključevima
- TKIP (zasnovan na RC4 (WPA, WPA2)
  - Može da radi sa starijim hardverom
  - Rješava sigurnosne probleme WEP-a
- AES primjena zahtijeva novi hardver (WPA2)