SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

Bežične mreže

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

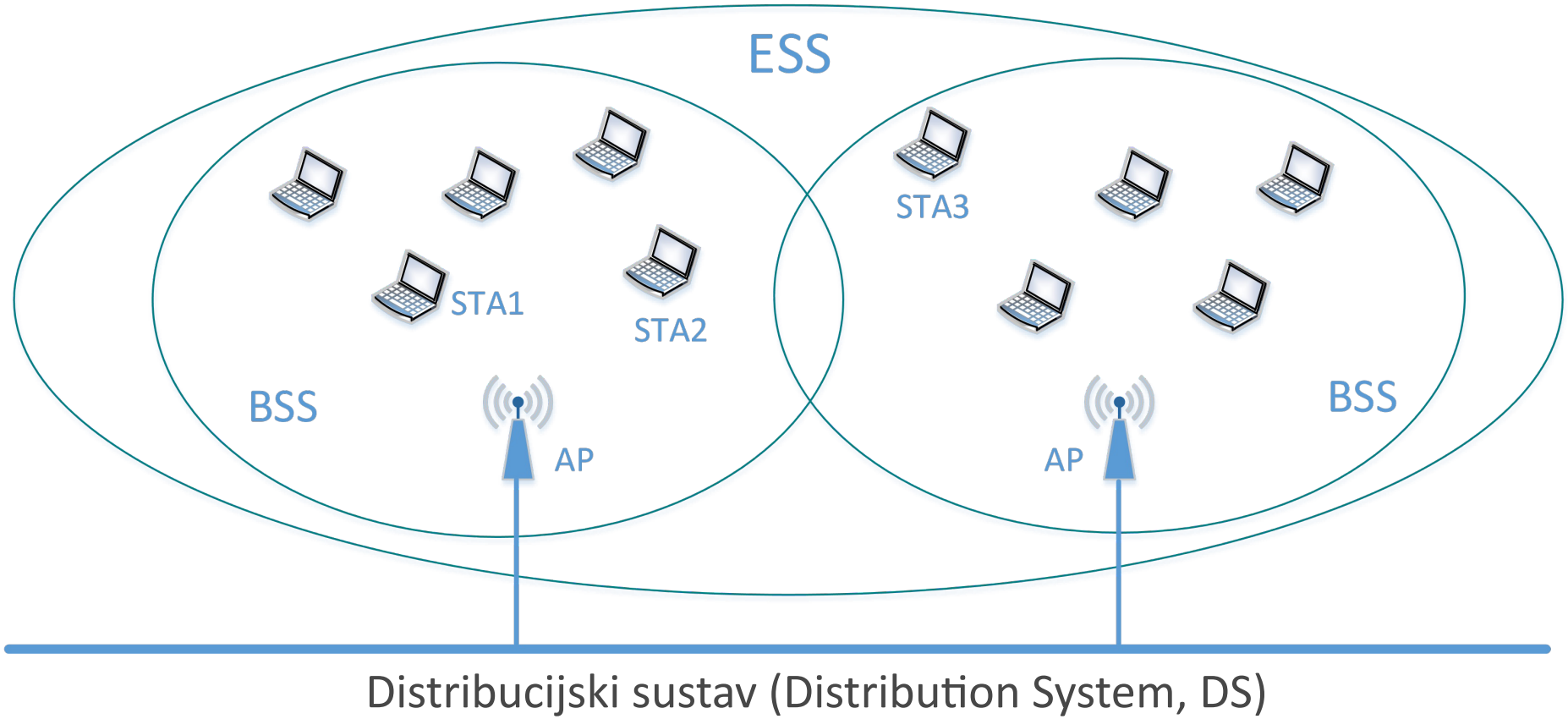
Sadržaj

- osnovno o bežičnim mrežama
- karakteristike Wi-Fi/802.11 bežičnih mreža
- 802.1x i EAP
- napadi na WPS, WPA i PSK/WPA Enterprise
- sigurnost u mobilnim mrežama

Osnovna svojstva bežičnih mreža

- bežične mreže koriste elektromagnetske valove za prijenos podataka
  - po prirodi je vrlo teško ograničiti pristup mediju
- mnoštvo je različitih bežičnih mreža
  - u ovom dijelu bavit ćemo se sa 802.11
  - kasnije u predmetu bit će riječi o Bluetooth i o mobilnim mrežama iz perspektive mobilnih uređaja
- dva osnovna načina rada 802.11: ad-hoc i infrastrukturni
  - Ad-hoc (IBSS, Independent Basic Service Set) omogućava direktnu komunikaciju stanica
  - u infrastrukturnom načinu rada koristi se pristupna točka (AP) preko koje svi komuniciraju

Arhitektura 802.11 u infrastrukturnom načinu



- STA – *station*, stanica
- AP – *access point*, pristupna točka

Neki dodatni pojmovi

- pojedina pristupna točka identificirana je s BSSID parametrom (engl. Basic Service Set Identifier)
  - najčešće jedna od MAC adresa pristupne točke
- skup pristupnih točaka identificiran je ESSID-om (ili kraće SSID-om) (engl. Extended Service Set ID)
  - identifikacijski niz maks. duljine 32 znaka
  - nije namijenjen kontroli pristupa; objavljuje se u tzv. Beacon upravljačkim okvirima
- zbog karakteristika medija sigurnost bežičnih mreža značajno se temelji na kriptografiji!

BSS - Basic Service Set

- jedna pristupna točka (AP), oglašava SSID (kao naziv mreže za taj BSS)
- klijenti se spajaju na AP
- fizička dostupnost signala: BSA (Basic Service Area)
- AP je u pravilu „uplinkom” spojen na Ethernet

ESS - Extended Service Set

- više pristupnih točaka (Access Points) koje imaju isti SSID (a različite BSSID) povezano na komutator (switch)
- korisnik može prelaziti iz područja signala jednog AP u drugi bez raskidanja komunikacije (*roaming*)

802.11 porodica bežičnih mreža

- lokalna bežična mreža temeljena na protokolu Ethernet

IEEE standard	Max brzina	Frekvencija	Napomena
802.11 (1997)	2 Mbps	2.4 GHz	Inicijalna verzija koja se više ne koristi
802.11a (1999)	54 Mbps	5 GHz	Nekompatibilna s b i g standardima
802.11b (1999)	11 Mbps	2.4 GHz	Često korištena tehnologija zbog starije opreme
802.11g (2003)	54 Mbps	2.4 GHz	Često korištena tehnologija zbog starije opreme
802.11n (2009)	600 Mbps	2.4 GHz / 5 GHz	Najčešće korištena varijanta
802.11ac (2014)	7 Gbps	5 GHz	Najnoviji, sve više u upotrebi
802.11ax (2021)	9.6 Gbps	2.4 / 5 / 6 GHz	„Wi-Fi 6“ (6. verzija standarda 802.11)

Protokoli za sigurnost bežičnih mreža (1)

- za sigurnost bežičnih mreža definirani su WEP, WPA, WPA2 i WPA3
  - WPA (Wi-Fi Protected Access) je komercijalni i zaštićeni nazivi Wi-Fi udruge
  - IEEE definira 802.11i normu i u sklopu nje RSN („Robust Security Network”) i TSN („Transitional Security Network”)
- WEP definiran 1999. godine
  - školski primjer kako ne upotrebljavati kriptografiju
- WPA uveden 2003. godine kao privremena mjera
  - baziran na draftu 802.11i specifikacije
  - bilo je nužno podržati postojeću opremu koja je omogućavala WEP
- WPA2 definiran 2004. godine

Protokoli za sigurnost bežičnih mreža (2)

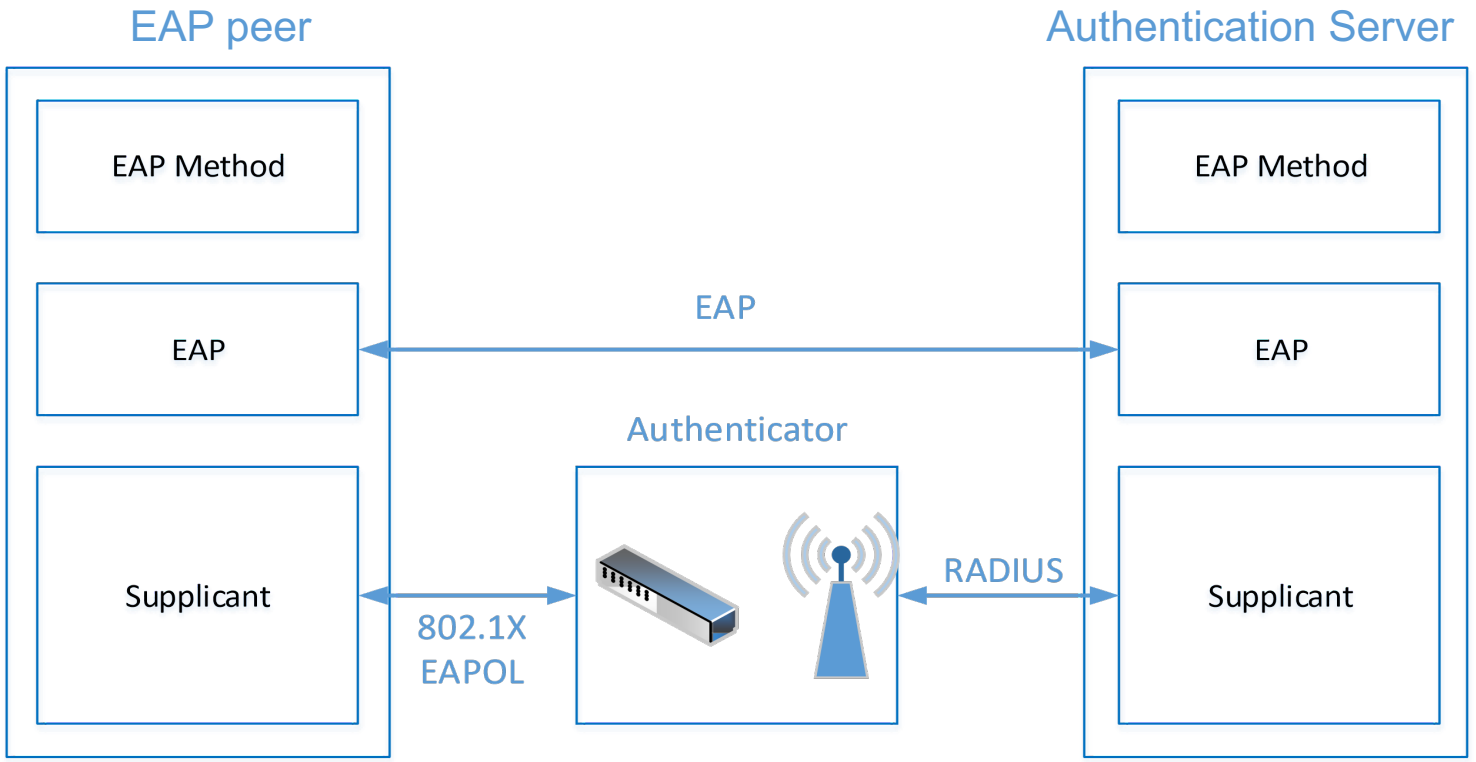
- WPA3 definiran u 7. mjesecu 2018. godine
  - poboljšana zaštita prilikom korištenja nedovoljno kompleksnih lozinki
    - Simultaneous Authentication of Equals (SAE)
  - dijeljena tajna u WPA3-Personal se više ne može jednostavno pogađati
  - uklonjeni kripto algoritmi koji se smatraju nesigurnima
  - uvedena zaštita upravljačkih okvira (Protected Management Frames, PMF)
  - uvodi ključeve veličine 192-bita u WPA Enterprise inačicu
    - dodatne zaštite za prijenos osjetljivih informacijama u okruženjima kao što su financijske ili vladine institucije.
  - Wi-Fi CERTIFIED Easy Connect – spajanje na mrežu jednostavnih uređaja (IoT uređaji) upotrebom nekog složenijeg uređaja (primjerice, mobilnog telefona)
    - zamjena za WPS

Kontrola pristupa bežičnoj mreži

- WPA/WPA2/WPA3 PSK
  - PSK – pre-shared key, dijeljena tajna
  - autentifikacija se temelji na dijeljenoj tajni veličine 8-63 ASCII ispisiva znaka
  - prednosti
    - jednostavna za postavljanje
  - nedostatci
    - u slučaju odlaska zaposlenika dijeljena tajna se mora mijenjati na svim uređajima
    - efektivno se radi o lozinci što znači da se mogu provoditi napadi koji se provode na njih
- WPA/WPA2/WPA3 Enterprise
  - centralizirana autentifikacija koju obavlja poseban poslužitelj (Radius)

Arhitektura autentifikacije temeljene na EAP-u

- koristi se isključivo u WPA[23] Enterprise varijanti
  - potrebno je imati poseban autentifikacijski poslužitelj (Radius ili Diametar)



EAP i 802.1x

- EAP: Extensible Authentication Protocol
- generički sustav mrežne autentifikacije (RFC3748)
- definira četiri tipa poruka: request, response, success, failure
  - ne definira kako se poruke prenose niti konkretne metode autentifikacije
- dodatno se definiraju autentifikacijske metode
  - ima ih preko 40, standardnih i nestandardnih
  - neke metode su slabe, neke omogućavaju autentifikaciju samo klijenta, a neke jake i omogućavaju autentifikaciju i klijenta i poslužitelja
- za prijenos EAP poruka preko Etherneta u 802.1x-2010 je definiran protokol EAPOL
  - pokriva niz različitih mreža, ne samo 802.11

Radius - Remote Authentication Dial-In User Service

- mrežni protokol za centralizirani AAA (authentication, authorization, accounting) za korisnike koji pristupaju i koriste mrežne usluge
- model klijent/poslužitelj (u pravilu UDP, može i TCP)
- „back-end” za autentifikaciju 802.1X
- korisnik (ili uređaj) šalje NAS poslužitelju (Network Access Server) zahtjev za pristup određenom mrežnom resursu korištenjem svojih pristupnih vjerodajnica (*access credentials*)
  - šalje se nekim protokolom podatkovne veze, na primjer PPP (Point-to-Point Protocol) ako se radi o "dialup" ili xDLS pružatelju usluge ili se koristi HTTPS post kroz web forme

Radius (2)

- komunikacija NAS i Radius poslužitelja treba biti dodatno zaštićena na primjer IPsec tunelom
  - lozinka je zaštićena dijeljenom tajnom i MD5 algoritmom
- RADIUS poslužitelj provjerava informacije korištenjem autentifikacijskih shema tipa PAP, CHAP ili EAP
- verificira se identitet korisnika, adresa, broj telefona, stanje računa, dozvole za pristup mrežnim uslugama
- korisnički podaci: lokalne datoteke (nekad), danas SQL, LDAP, Active Directory, ...

Radius (3)

- NAS šalje RADIUS poslužitelju poruku "Access Request"
  - sadrži pristupne vjerodajnice, tipično u obliku username/password ili korisničkog certifikata
  - dodatno se mogu nalaziti podaci o korisniku poznati NAS-u (mrežna adresa, broj telefona, podaci o fizičkom priključku)
- RADIUS poslužitelj odgovara:
  - Access Reject
  - Access Challenge (dodatna lozinka, PIN, token, kartica) ili uspostava sigurnog tunela između korisnika i Radius poslužitelja
  - Access Accept

Radius (4)

- RADIUSaaS - Radius as a service
  - jednostavna i sigurna autentikacija za pristup mrežnim resursima
  - autentifikacija se temelji na klijentskim certifikatima
  - provjera opozvanih certifikata (OCSP)
  - generiranje konfiguracijskih profila

- Diameter
  - nadogradnja Radiusa, nije direktno kompatibilan
  - podrška za TCP i SCTP
  - pregovaranje mogućnosti
  - definirani mehanizmi za "failover"
  - mogućnost proširenja i nadogradnji
  - zaštita na transportnom sloju (TLS ili IPsec)

Fizički sloj

- na fizičkom sloju definiraju se radio karakteristike
  - frekvencije, snaga, modulacije
- koristi se nelicencirani spektar 2.4 GHz i 5 GHz (6 GHz)
  - smetnje od drugih uređaja
- oblikom i razmještajem antena te snagom može se utjecati na pokrivenost
  - to ne znači da napadač ne može koristiti specijalnu opremu kako bi pristupio bežičnoj mreži s veće udaljenosti

Vrste okvira i njihova zaštita

- u 802.11 bežičnim mrežama upotrebljavaju se tri vrste okvira:
  - podatkovni okviri – prenose korisničke podatke
  - upravljački okvir – upravljanje MAC-om
    - uspostavljanje asocijacije, reasocijacija, odspajanje, autentifikacija, beacon…
  - kontrolni okviri – upravljanje pristupom mediju
    - RTS, CTS, ACK, …
- samo podatkovni okviri su kriptografski zaštićeni
  - norma 802.11w ratificirana 2009. godine omogućava zaštitu upravljačkih okvira
    - nije dostupno u svoj opremi
    - nije moguće zaštiti sve okvire (npr. Beacon), odnosno općenito sve koji se koriste prije prijave

Napadi uskraćivanjem usluge

- RF ometanje (engl. RF jamming)
  - Queensland Attack (kontinuirano slanje jakog signala)
- virtualno ometanje (engl. Virtual jamming)
  - manipulacija RTS/CTS okvirima
- lažiran zahtjev za odspajanjem (engl. spoofed disconnect)
- Connection request flooding

Napadi na kriptografiju

- WEP: školski primjer krive upotrebe kriptografije
  - uz pomoć gotovih alata (aircrack-ng) vrlo jednostavno je moguće doći do dijeljene tajne (potrebno je snimiti oko 50 k okvira)
  - nakon toga moguće je pristupiti mreži bez ikakvih problema
- WPA ima određenih problema
  - algoritam za zaštitu integriteta, Michael, nije dovoljno jak. U prosjeku nakon 2^{28} pokušaja moguće je lažirati sadržaj poruke
  - kad se detektira krivi MIC (message integrity check) AP pretpostavlja da je u pitanju aktivni napad i:
    - obavlja bilježenje sigurnosnog incidenta, blokira stanicu u slučaju 2 pogreške u 60s, mijenja PTK i GTK, blokira port
- WPA2 ima ranjivost KRACK (Key Reinstallation Attack)
  - https://www.krackattacks.com

Nekriptografski napadi na WPA i WPA2

- WPA PSK ranjiv na pogađanje dijeljene tajne
- uz pomoć deautentifikacijskih napada moguće snimiti autentikaciju
- potom off-line pogađanje lozinki
  - na CPU, rješenja za GPU, korištenje Cloud usluge
- PSK je moguće otkriti i kompromitiranjem klijenata
- PSK omogućava spajanje na mrežu, ali ne i dešifriranje snimljenog prometa
  - potrebno je znati PTK (engl. pairwise transit key)

Napadi na WPA2 Enterprise

- ranjivost ovisi o konkretnoj upotrijebljenoj EAP metodi
  - u RFC4017 definirane preporuke za EAP metode koje se koriste u bežičnim mrežama
- EAP-MD5, EAP-LEAP
  - podložni pogađanju lozinke, ne omogućava međusobnu autentifikaciju (MITM)
  - mora ih se koristiti sa nekakvom dodatnom zaštitom
- EAP-TLS, EAP-TTLS
  - sigurni, ali je potencijalni problem neodgovarajuće rukovanje certifikatima

iOS Wi-Fi poruka „weak security”

- WPA koristi TKIP (Temporal Key Integrity Protocol)
  - ne smatra se sigurnim od 2009.
- WPA2 koristi CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
  - sigurniji, temelji se na AES
- napad na mrežu WPA + TKIP:
  - neki klijent mora biti spojen
  - izvede se deautentifikacija i dohvaća razmjena ključeva („four-way handshake”)
  - ugrađeno u aircrack-ng, pretraga rječnika dok se ne pronađe ključ
- WPA2
  - „deauthentication” okviri nisu šifrirani
  - DoS napad (ne može se spriječiti)
  - Rogue access point (Evil Twin Attack)

WPS - Wi-Fi Protected Setup

- jednostavan mehanizam za konfiguriranje „sigurne” bežične mreže
  - za autentifikaciju pristupne točke i klijenta
- olakšava podešavanje WPA PSK zaštite
  - korisnik na računalu upiše 8-znamenkasti PIN zapisan na kućnom usmjerniku
  - usmjernik pošalje dobru dijeljenu tajnu računalu i na dalje se upotrebljava WPA PSK
- ranjivost (u dizajnu) bitno ograničava prostor mogućih vrijednosti
  - „brute force” napad može otkriti PIN za 4-10 sati
  - neovisno o korištenom šifriranju
- problem je što se radi samo o 8 znamenkastom broju
  - gdje je zadnja znamenka kontrolna
  - i znamenke se prenose u grupama 4+3 pri čemu AP daje odgovor već nakon prve grupe
  - dakle, potrebno je samo 11000 pokušaja ($10^4 + 10^3$, umjesto inicijalno zamišljenih 10^8)

Neovlaštene i otvorene pristupne točke

- neovlaštene pristupne točke (engl. Rogue access points)
  - može ih postaviti neki djelatnik u želji da si olakša pristup mreži
  - pristupne točke dolaze u raznim formatima – postoje USB verzije koje se mogu priključiti na prijenosna/stolna računala
  - napadač koji se pokušava ubaciti u komunikaciju ili dohvatiti inicijalnu razmjenu radi vjerodajnica
  - Evil Twin Attack, napadač doda AP s istim ESSID kao legitimna pristupna točka
- otvorene pristupne točke na javnim mjestima ili u kafićima
  - problematične jer mogu biti namjerno podmetnute
  - ako nisu podmetnute, na tim otvorenim mrežama može se nalaziti napadač vrebajući žrtve

Neke preporuke za sigurnost bežičnih mreža

- ne koristiti ako nije nužno
- ako se mora koristiti
  - upotrebljavati WPA3 Personal ili Enterprise verzije ako je ikako moguće
  - koristiti složene lozinke koje nije jednostavno pogoditi
  - upotrebljavati WPA2 Enterprise verziju
  - u slučaju WPA2 Enterprise paziti na korištenje odgovarajućih EAP metoda
  - ne koristiti WPS

- Wi-Fi Protected Access® Security Considerations (May 2021)
  https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security_Considerations_20210511.pdf