Pitanja sigurnosti radijskog umrežavanja

Igor Bartolić, dipl. ing.

Sadržaj

- Uvod
- *Pojmovi u WLAN sigurnosti*
  - WEP
  - WPA/WPA2
  - Radius poslužitelj
  - PSK
  - 802.1x/EAP
  - PEAP
  - PEAP-EAP-TLS
  - TTLS (EAP-TTLS)
  - TKIP MIC
  - AES-CCMP
  - PKI

Sadržaj

- Podjela sigurnosti
- Sigurnost od vanjskih napada:
  - Osobna i uredska sigurnost
  - Sigurnost manjih kompanija
  - Sigurnost srednjih i velikih kompanija
  - Vojna (najveća) sigurnost
  - Zaključak
- Sigurnost od unutarnjih napada
  - Metode zaštite
- Zaključak
- Vaša pitanja

Uvod

- Nekoliko riječi o predavaču
- WLAN – Radijske pristupne mreže

Pojmovi u WLAN sigurnosti - WEP

WEP (*Wired Equivavalent Privacy*)

Samo ime nije nikad opravdano (privatnost kao u fiksnim mrežama)

1) 64-bit WEP (40 bit *shared secret* + 24 bit IV)
2) 128-bit WEP (104 bit *shared secret* + 24 bit IV)
3) WEP2 – 128 bit IV

IV (*Initalization Vector*) – broj koji se stalno mijenja
- u kombinaciji sa *shared secretom* – šifrira podatke

Velike slabosti:

1) Isti IV se koristi više od jednom
2) S 24 bitnim IV-om samo 16,7 milijuna kombinacija
3) Koristi se stalni, a ne privremeni ključevi
4) Većina korisnika ne mijenja svoje ključeve

WPA

WPA (*Wi-Fi Proteced Access*)

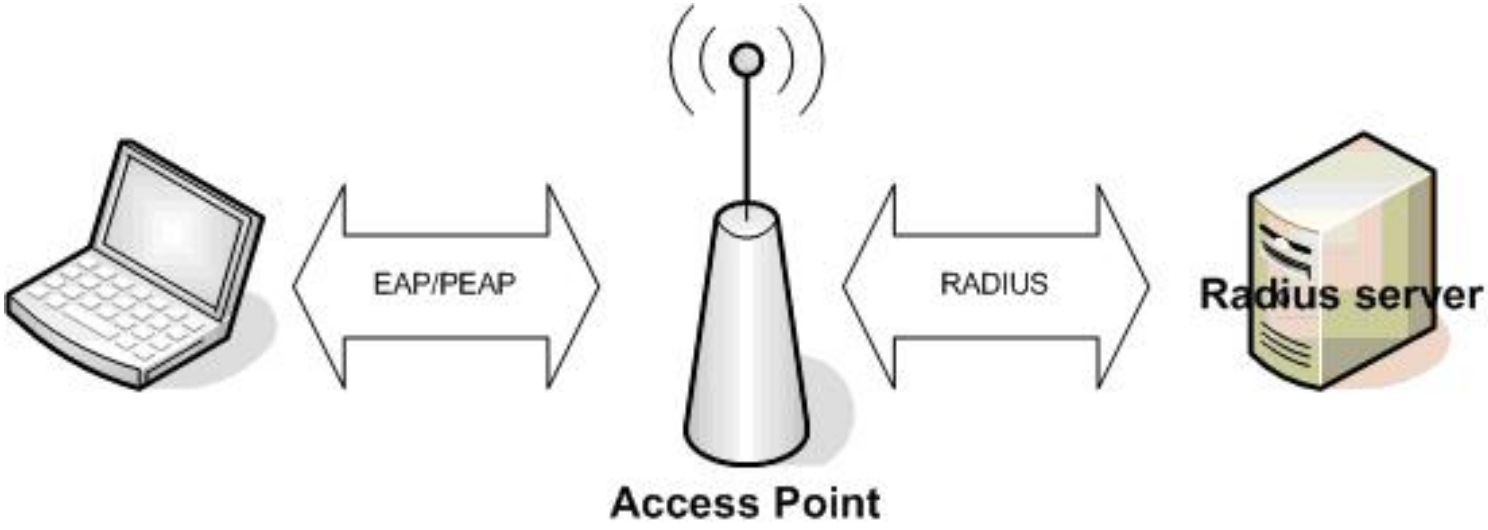
- Korporacijski (*Enterprise*)
- Osobni (*Personal*)

	WPA	WPA2
Enterprise	Authentication: 802.1X/EAP Encryption: TKIP/MIC	Authentication: 802.1X/EAP Encryption: AES - CCMP
Personal	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES - CCMP

RADIUS

RADIUS (*Remote Authentication Dial In User Service)* poslužitelj

- AAA (*Authentication, Authorization and Accounting*)
- Microsoft – IAS (*Internet Authentication Server*)
- Juniper – Steel Belted Radius
- Redback – NetOp Policy Manager
- FreeRADIUS – Linux – Open Source



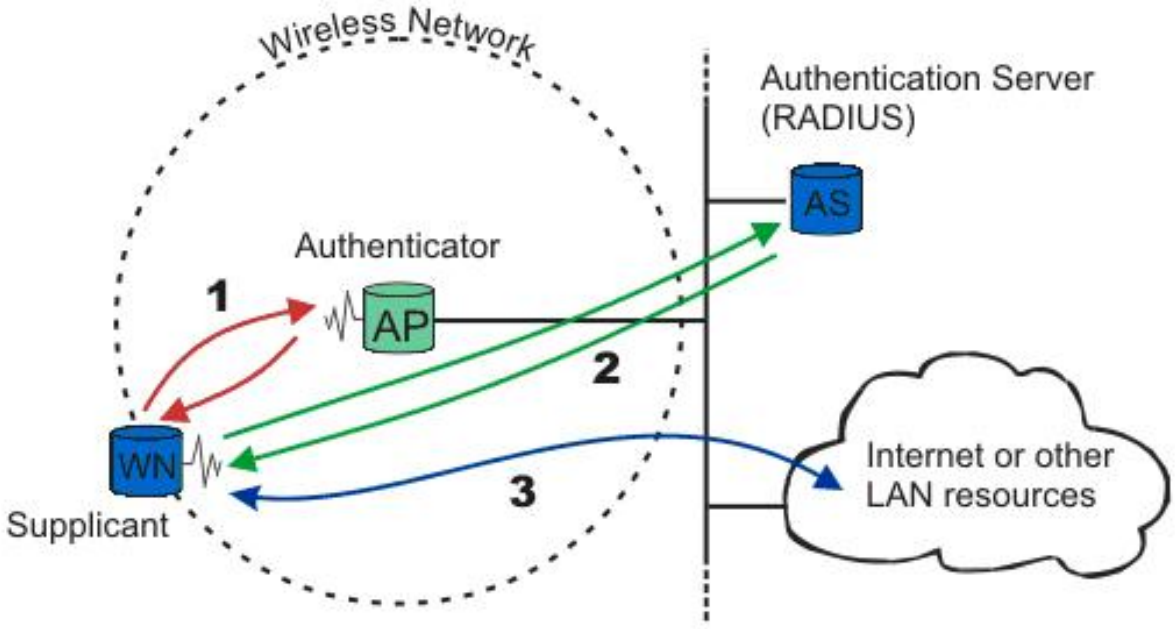
PSK

PSK (*Pre-Shared-Key*)

- WPA autentikacija kada nije dostupan Radius poslužitelj
- šifriranje pomoću 256 bitnog ključa
- u komunikaciji između AP (pristupne točke) i klijenta nikada se ne koristi originalni ključ
- koristi se privremeni ključ koji se generira iz privatnog ključa

802.1x/EAP

802.1x/EAP (*Extensible Authentication Protocol*)

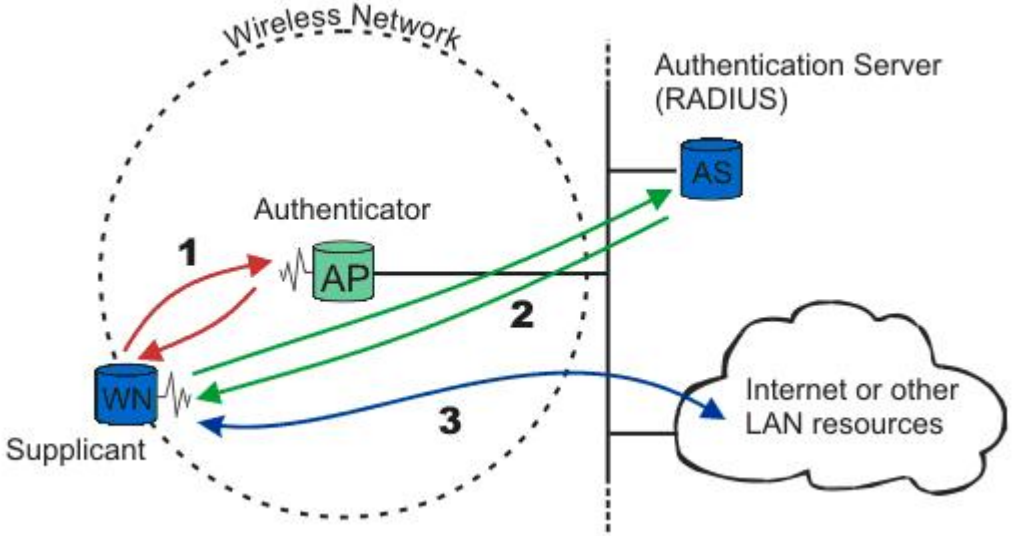


3 entiteta uključena u autentikaciju:

1) Authenticator (AP)
2) Supplicant (SW na PC-u klijenta)
3) Authentication Server (RADIUS)

802.1x/EAP - nastavak

802.1x/EAP (*Extensible Authentication Protocol*)



Ako se pojavi novi klijent u mreži– Authenticator mu otvori port, koji je u neautoriziranom stanju

1) Authenticator pošalje EAP zahtjev prema Supplicantu.
   Supplicant odgovara EAP odgovorom
2) Authenticator prosljeđuje EAP odgovor prema Authentication poslužitelju.
   Ako Authentication poslužitelj prihvati zahtjev, Authenticator njegov port stavlja u stanje dozvoljenog pristupa.
3) Kada Supplicant dobije pristup, dozvoljen mu je normalan promet.

PEAP (*Protected EAP*)

PEAP (*Protected Extensible Authentication Protocol*)

- izgovara se "peep"
- razvili su ga Cisco, Microsoft, RSA Security
- nije samo autentikacijski protokol (kao druge vrste EAP-a)
- koristi "server-side public certificate"
- formira šifrirani SSL/TLS tunel između klijenta i autentikacijskog poslužitelja
- ključ za šifriranje se prenosi koristeći "server's public key"
- razmjena autentikacijskih informacija prenosi se preko šifriranog tunela
- sličan EAP-u

PEAP - nastavak

2 vrste PEAP-a:

- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC

PEAPv0/EAP-MSCHAPv2

- najčešći oblik PEAP-a
- unutarnji autentikacijski protokol je Microsoft's Challenge Handshake Authentication Protocol

PEAPv1/EAP-GTC

- kreirao ga je Cisco, ali ne i Microsoft (Windows OS ga ne podržava)
- interoperabilnost s postojećim token karticima i directory autentikacijskim sustavima

PEAP-EAP-TLS

PEAP s EAP-TLS

- TLS (Transport Layer Security)
- koristi certifikat na poslužitelj (RADIUS) strani
- klijenti moraju imati ili certifikate ili "smart card"
- mora se koristiti PKI (*Public Key Infrastructure*)

TTLS (EAP - TTLS)

TTLS ili EAP – TTLS

EAP – *Tunneled Transport Layer Security*

- razvili su ga Funk Software i Certicom
- za razliku od Linuxa, za Windows potrebna instalacija dodatnog programa
- jako dobra sigurnost s time da klijenti ne trebaju imati na sebi certifikate
- kada je poslužitelj autenticiran na klijent – kriptirani tunel – preko kojega se autenticira klijent
- korisničko ime (*username*) se nikada ne prenosi bez sigurnosnog tunela

TKIP s MIC

TKIP (*Temporal Key Integrity Protocol*)
u odnosu prema WEP-u donosi:

- nova metoda generacije ključa sesije (*session key*), tako da se PSK nikada ne koristi, nego se iz njega generira ključ sesije, koji se konstantno mijenja; pomoću tog promjenjivog ključa sesije šifriraju se podaci
- mehanizam provjere integriteta podataka (MIC, *Message Integrity Check*)

2 faze šifriranja:

1) Generira se ključ sesije od privremenog ključa, TKIP brojača i MAC adrese pošiljatelja
2) Od sesijskog ključa šifriraju se podaci

TKIP s MIC - nastavak

MIC - Mehanizam provjere integriteta podataka (*Message Integrity Check*)

- zovu ga i **Michael**

Ako se u 60 s dogode 2 MIC pogreške - AP se automatski ugasi na 60 s i *boota* te nakon toga klijenti moraju promijeniti ključeve

Kako se ne bi dogodilo da paketi izobličeni od interferencije stalno ruše AP: prije nego se poveća MIC brojač za zaštitu rade se sljedeće provjere:

- FCS (*Frame Check Sequence*)
- TKIP *sequence counter*

Ako paket padne na tim provjerama, ne uvećava se MIC brojač za zaštitu

AES - CCMP

AES (*Advanced Encryption Standard*)

- neobavezan u WPA, ali obavezan u WPA2
- šifriranje pomoću 128 bitnog ključa

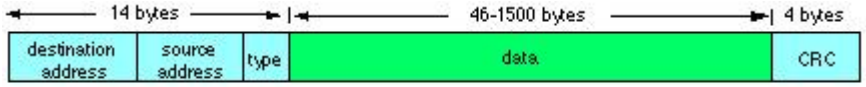
CCMP

(*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)

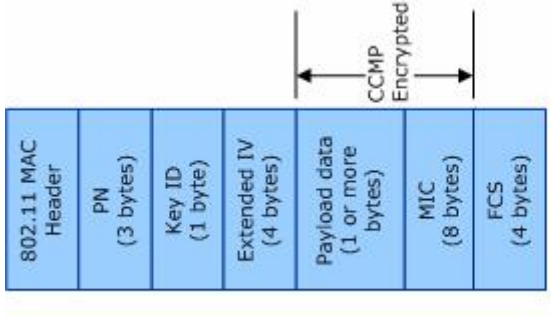
- integritet podataka – MIC
- PN (*packet number*) nalazi se u CCMP zaglavlju – uključeno je u šifriranje i MIC proračun

AES – CCMP zaglavlje

Normalan MAC paket

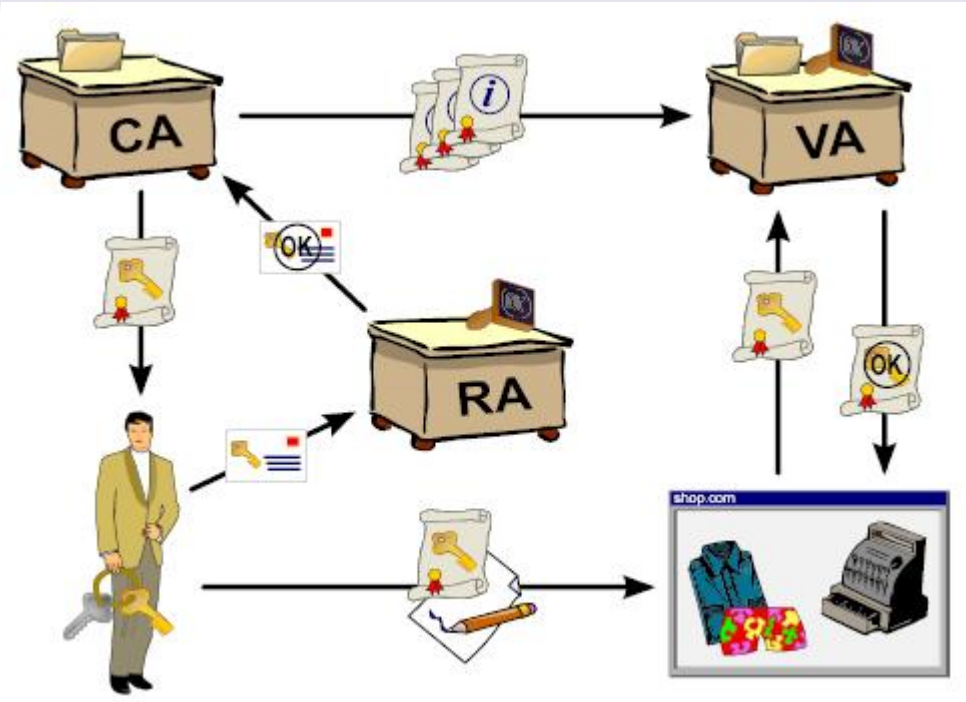


AES-CCMP MAC protocol data unit (MPDU)



1. **PN** *packet number* – služi za "replay protection"
2. **ID *key Identifier*** bit 7,6 – indeks ključa 0-3, bit 5 – prošireni IV, bit 4-0 – 0
3. **Prošireni IV** – sadrži bajtove PN
4. **Payload data**
5. **MIC -** AES-CCMP izračunava MIC vrijednost Payload data
6. **FCS** – *Frame Check Sequence* – 32 bitni CRC (*Cyclic Redundancy Code*) izračunat iz svih podataka iz MPDU-a

PKI (*Public Key Infrastructure*)



PKI (Public key infrastructure) softver, hardver, ljudi, procedure potrebni da se kreiraju, upravljaju, pohranjuju, distribuiraju, i ukidaju digitalni certifikati

CA – *Certificate Authority*
RA – *Registration Authority*
VA – *Validate Authority*

CA – proces izdavanja i registracije javnog ključa korisnicima - svaki korisnik mora biti jedinstven

RA – osigurava to povezivanje javnog ključa s određenim korisnikom

Certifikat javnog ključa - identitet korisnika, javni ključ, njihova veza, ispravnost - izdan od CA

VA – osigurava i provjerava ispravnost certifikata

Podjela sigurnosti

Sigurnost od vanjskih i unutarnjih napada

Sigurnost od vanjskih napada:

1. Osobna i uredska sigurnost
2. Sigurnost manjih kompanija
3. Sigurnost srednjih i velikih kompanija
4. Vojna (najveća) sigurnost

Osobna i uredska sigurnost

Level 1: *Home and SOHO WLAN Security*

- promijeniti unaprijed postavljeni (*default*) SSID (*Service Set Identifier*)
- isključiti *broadcast* SSID
- staviti WPA, ne koristiti WEP
- većina opreme samo s upgradeom firmwarea na AP i upgradeom OS-a i pogonskih programa (*drivers*) na WLAN kartici
- uključiti MAC filtriranje
- WPA – probijen s TKIP šifriranjem i to sa slabim PSK
- PSK treba biti složen (ne iz rječnika, već kombinacijom velikih i malih slova, brojeva, znakova)

Network Stumbler

Sigurnost manjih kompanija

Level 2 - *Small Business WLAN Security*

– razina iznad kućne sigurnosti

Uvođenje autentikacije:

1) PEAP
2) TTLS

PEAP – radi se o PEAP-EAP-MSCHAPv2 koji zahtjeva digitalni certifikat na poslužitelj strani i na klijent strani *username/password*

TTLS – sigurnija verzija od PEAP-a jer se ni korisničko ime ne prenosi nešifrirano

Potreban je RADIUS poslužitelj

RADIUS u PEAP/TTLS modu mora imati x.509 certifikat (godišnje $500)

Sigurnost manjih kompanija - nastavak

Self Signed Digital Certificate – sami ste ga generirali na Radius poslužitelju

- nije po PKI proceduri – ali puno bolje nego koristiti autentikacije samo preko *username/password* (LEAP)

Najjednostavnije da se koristi **IAS** – **Windows 2003 Server**

- na istom poslužitelju imati i AD, IAS i CA
- pomoću Group Policy na AD-u – automatska instalacija certifikata javnog ključa (*public key certificate*)
- za TTLS na IAS-u Funk Software Odyssey server ($2000)

FreeRadius – LINUX – besplatno TTLS

- MDC

Sigurnosni rizici – dobivanje *passworda* od korisnika

- krađom, nagovaranjem, gledanjem preko ramena
- instalacija "key loggera" na korisničkom računalu
- veća sigurnost od velike većine fiksnih mreža

Sigurnost srednjih i velikih kompanija

Level 3 - *Medium to Large Enterprise WLAN Security*

- na temelju prethodne razine (Level 2) bez samostalnog izdavanja certifikata (*Self Signed Digital Certificates*)
- ne preporuča se ni korištenje PEAP-EAP-MSCHAPv2
- koristiti EAP-TLS ili PEAP-EAP-TLS
- koriste se **Soft Digital Certificate** – certifikati pohranjeni na hard disku korisnika
- isti kriteriji za certifikate i na korisničkoj i poslužiteljskoj strani
- poslužitelji predviđeni samo za potrebe zaštite – posebno za Radius, posebno za CA
- pridržavanje PKI procedure
- > 1000 ljudi – ljudi i infrastrukture samo za PKI
- certifikati od izgubljenih, ukradenih računala – poništiti - CRL
- CRL (*Certificate Revocation List*)

AD – ne izdavati automatski certifikate svim klijentima

- kreira se OU (*Organization Unit*) – Certificate OU
- korisnicima kojima je potreban pristup WLAN-u dodijeli se Certificate OU

Level 3 - nastavak

Šifriranje – minimum TKIP, ali preporuča se AES

Sigurnosni rizici - vrlo siguran

- nije dovoljna samo krađa username/password, nego i certifikata (puno puno manja vjerojatnost)
- jedino krađa čitavog PC-a – ali imamo PKI infrastrukturu – automatsko poništenje certifikata
- najveća mogućnost probijanja – *backdoor*, virus, worm (ali ako imate centraliziranu i automatsku kontrolu vaših računala mogućnst probijanja je minimalna)

Vojna (najveća) sigurnost

Level 4 - *Military Grade Maximum Level WLAN Security*

Temelji se na Level 3, uz smanjenu mogućnost krađe certifikata pomoću malicioznih programa

- PKI certifikat autoriteti – koriste se HSM (*Hardware Security Modul*) ($ nx1000) na CA
- svi PKI poslužitelji – nisu povezani ni međusobno ni s ostatkom mreže
- sva interakcija između PKI entiteta – ručno se obavlja

Digitalni certifikati ne smiju biti na hard diskovima

- koriste se -TLS ili PEAP-EAP-TLS s upotrebom hard tokena
- certifikati jedino na HSM-ovima na CA
- korisničko HSM-ovi - šifrirani tokeni – USB diskovi i smart-card
- krađom PC-a se ne dobiva certifikat
- ako se ukrade HSM – poništi se certifikat – dio redovnog PKI procesa
- danas postoje i HSM-ovi s biometrijom – čitač otiska prstiju – najjači mogući autentikacijski sustav

Level 4 - nastavak

Šifriranje – AES – jedino dozvoljen

- AP i WLAN kartice – samo 802.11i ili WPA2 certificirani
- korištenje najnovijih *firmwarea* i *drivera*

Sigurnosni rizici – Level 4 i nema neke slabe točke

- haker bi trebao uzeti i *password* i HSM, a da korisnik ne prijavi krađu
- ako imamo HSM-ove s čitačima otiska prstiju – praktički neprobojno

Zaključak

Zaključak

- WLAN može biti sigurniji i od fiksnih mreža
- "koliko para toliko muzike"
- oprema koju se koristi za WLAN šifriranje (RADIUS, PKI, HSM-ovi) – istodobno se mogu koristiti i za VPN i udaljeni pristup u fiksnom dijelu mreže

Sigurnost od unutarnjih napada

Sigurnost od napada vlastitih zaposlenika

"Divlje", *rogue*, WLAN mreže – najveća prijetnja WLAN sigurnosti
- AP, soft AP-ove (laptopi u ad-hoc modu), PC-ovi, radijski skeneri kodova, radijski printeri
- WLAN oprema je sada relativno jeftina
- zaposlenici koriste svoju privatnu opremu, kada je i IT odjel službeno i nema
- oprema bez ikakvih sigurnosnih standarda

Nestručno podešene WLAN stanice – veća sigurnosna rupa od AP-ova
- *defaultne* postavke WLAN kartica – laka meta za hakere

Nestručno podešeni AP-ovi
- *defaultne* postavke
- u dometu su susjednih WLAN mreža

Metode zaštite

Metode zaštite

- "ručno", tj. "nožno" – administrator se šeće uz upotrebu Network Stumblera
- 24/7 nadzor – WLAN oprema za nadzor
  - *wireless-intrusion detection*
  - *real-time* mogućnost detekcije
- Zaključavanje sve WLAN opreme
  - svaki PC s WLAN karticom mora imati osobnog agenta koji će upozoriti organizaciju i korisnika na sigurnosne rupe
  - organizacije moraju postaviti AP-ove po razinama koje sam prije spomenuo
  - obavezna promjena *defaultnih* postavki
  - ukinuti *broadcast* SSID
  - zabrana spajanja na manjim brzinama

Metode zaštite - nastavak

- *Intrusion Detection and Protection*
  - IDP sustavi specijalizirani za WLAN mreže – *real-time* praćenje 802.11a/b/g protokola
  - stalno praćenje WLAN napada, protokol analiza, statistika sumnjivog prometa
  - mogućnost detekcije WLAN napada prije nego probiju sustav zaštite

Zaključak

Zaključak

- milijuni dolara uloženi u *firewalle*, IDP uređaje koji se brinu za sigurnost vaše fiksne mreže mogu biti bačeni ako ne primijenite dosad spomenute WLAN sigurnosne metode i 24/7 nadzor WLAN prometa

Zanimljive web-stranice

- http://www.home-wlan.com/
- http://www.wikipedia.org/
- http://www.lanarchitect.net/
- http://www.computerworld.com/