Sigurnost računalnih sustava

Mrežna sigurnost

- sigurnost bežičnih mreža (WiFi)

doc. dr. sc. Ante Đerek
doc. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Sigurnost bežičnih mreža

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
  - 802.11, mobilne mreže, Bluetooth, …
- Dva osnovna načina rada 802.11: ad-hoc i infrastrukturni
  - Ad-hoc način rada omogućava direktnu komunikaciju stanica
  - U infrastrukturnom načinu rada koristi se pristupna točka (AP) preko koje svi komuniciraju

802.11 porodica bežičnih mreža

- Lokalna bežična mreža temeljena na protokolu Ethernet

IEEE standard	Maks. 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

Protokoli za sigurnost bežičnih mreža (2)

- WPA2 definiran 2004. godine
- WPA3 definiran u 7. mjesecu 2018. godine
  - Poboljšana zaštita prilikom korištenja nedovoljno kompleksnih lozinki
    - Simultaneous Authentication of Equals (SAE)
    - Dijeljena tajna u WPA2-Personal se više ne može jednostavno pogađati
  - Uklonjeni kripto algoritmi koji se smatraju nesigurnima
  - Uvedena zaštita upravljačkih okvira (Protected Management Frames, PMF)
  - ključevi 192-bita u WPA Enterprise inačici
    - 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 (Wi-Fi Protected Setup)

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
  - Prednost: jednostavno postavljanje
  - Nedostatci:
    - U slučaju odlaska nekog 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

Fizički sloj

- Na fizičkom sloju definiraju se radio karakteristike
  - Frekvencije, snaga, modulacije
- Koristi se nelicencirani spektar centriran na 2.4 GHz i 5 GHz
  - Neke bežične mreže rade na 60 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 50k okvira)
  - Nakon toga moguće je pristupiti mreži bez ikakvih problema
- WPA ima određenih problema
  - Korišteni algoritam za zaštitu integriteta nije dovoljno jak te je u prosjeku nakon 2^{28} pokušaja moguće lažirati sadržaj poruke
  - Kod neuspješne provjere integriteta pretpostavlja se da je u pitanju aktivni napad:
    - AP zabilježi sigurnosni incidenta, blokira stanicu u slučaju 2 pogreške u 60s, mijenja ključeve, blokira port
- WPA2 ima ranjivost KRACK

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 ključ PTK („Pairwise Transient Key”)

Napad na sustav WPS

- WPS (engl. Wi-Fi Protected Setup) napravljen kako bi se olakšalo podešavanje WPA PSK zaštite
  - Korisnik na računalu ukuca 8-znamenkasti PIN zapisan na kućnom usmjerniku
  - Usmjernik pošalje dobru dijeljenu tajnu računalu i na dalje se upotrebljava WPA PSK
  - Postoje još neki mehanizmi koji se uglavnom ne koriste
- Problem:
  - radi se o samo 8 znamenkastom broju …
  - a zadnja znamenka je kontrolna …
  - i znamenke se prenose u grupama 4+3, pri čemu AP daje odgovor već nakon prve grupe.
  - Dakle, potrebno je samo 11000 (10^4+10^3) pokušaja (od početnih 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
- 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