FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Seminarski rad iz predmeta Sustavi za praćenje i vođenje procesa

Sigurnost WEP algoritma

Neda Živčić, 0036381301

Zagreb, lipanj 2005.

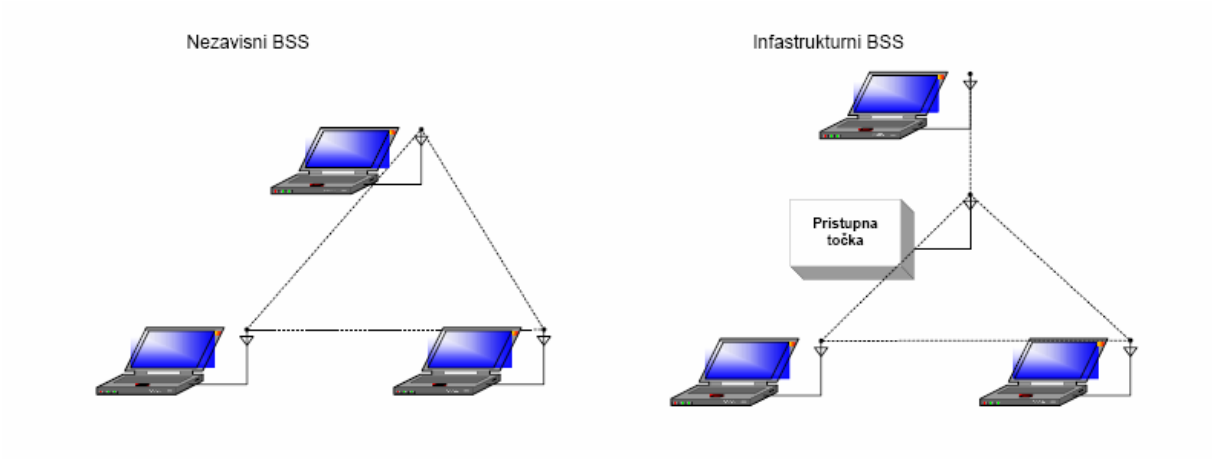
1. Uvod

Bežične mreže, zahvaljujući svojoj jednostavnosti implementacije i mobilnosti, postaju sve češće i sve popularnije. Upravo zbog tog porasta popularnosti i broja korisnika njihova sigurnost i upravljanje postaju sve veće pitanje koje traži sve bolje odgovore. Budući da su bežične mreže dijeljeni medij, postoji opasnost od presretanja svih poslanih i primljenih podataka. Zato se uvijek u obzir uzimaju postupci kodiranja (enkripcije), te potvrde vjerodostojnosti (autentifikacije) podataka. Pri implementaciji enkripcije i autentifikacije podataka moraju se razmotriti:

- korisnikova potreba za privatnošću: strogost protokola i cijena implementacije
- jednostavnost upotrebe: ako je implementacija pretjerano komplicirana, neće se koristiti
- vladine regulacije: enkripcija se u mnogim zemljama od strane vlade gleda kao oružje.

2. 802.11 standard

Standard 802.11. definira arhitekturu bežičnih mreža. Prema tom protokolu, osnovni element mreža je BSS *(engl .basic service set)* koji se sastoji od nekoliko stanica koje međusobno komuniciraju. Postoje dva oblika BSS-a, nezavisni i infrastrukturni, kako je prikazano na slici 1.



Slika 1. *Nezavisni i infrastrukturni BSS-ovi*

Kod nezavisnih BSS-ova (iBSS) mobilne stanice unutar jednog BSS-a međusobno izravno komuniciraju, te moraju biti unutar direktno dostupnog komunikacijskog područja. Unutar infrastrukturnih BSS-ova komunikacija se odvija preko pristupnih točaka (engl. *access point*). Pristupna točka je fizički povezana s fiksnom mrežom, dok je antenama povezana s uređajima koji koriste bežične mrežne kartice.

3. Wired Equivalent Privacy (WEP)

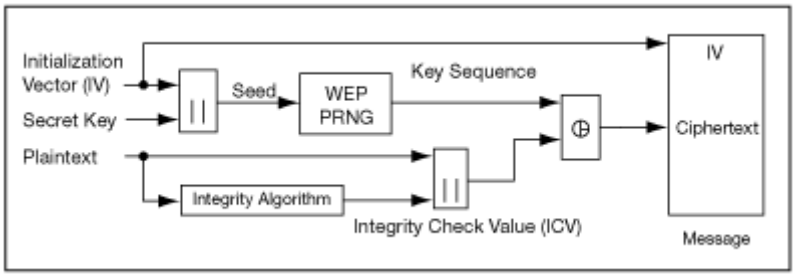
Wired Equivalent Privacy (WEP) je protokol ugrađen u 802.11 standard, koji služi za zaštitu podataka na podatkovnom sloju. WEP algoritmom se kriptira prijenos podataka između pristupne točke i klijenta. WEP pruža sigurnost na bežičnom dijelu veze, jer su mrežne kartice zadužene za kriptiranje 802.11 paketa pri slanju podataka, te za dekriptiranje prilikom primitka paketa podataka.

WEP algoritam pruža zaštitu podatka bežične komunikacije, ali na indirektan način spriječava neautorizirani pristup bežičnoj mreži. Iako ovo nije definirano 802.11 standardom, prevencija neautoriziranog pristupa se također smatra svojstvom WEP-a. Ovo je rezultat korištenja tajnih ključeva između mobilnih stanica i pristupne točke. Nepoznavanje dijeljenog tajnog ključa određuje mobilnu stanicu kao neautoriziranog korisnika.

WEP algoritam osmišljen je da bi odgovarao na slijedeće zahtjeve:

- razumna strogost (mora odgovarati potrebama korisnika),
- autosinkronizacija (stanice se određenom frekvencijom otkrivaju i sakrivaju),
- računalna efikasnost (moguća su programska i sklopovska rješenja),
- mogućnost izvoza (iz SAD-a u druge države),
- neobaveznost (nije obvezan da bi sustav ostao sukladan protokolu, korisnik odlučuje da li će koristiti WEP kriptiranje).

Način rada WEP algoritma je prikazan na slici 2.

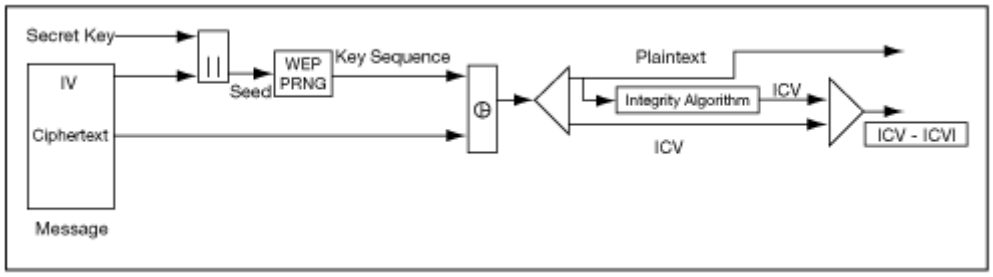


Slika 2. *WEP enkripcija*

WEP algoritam je simetrični algoritam, te se isti ključ koristi za enkripciju i dekripciju podataka. Izvorni paket podataka obrađuje se na dva načina: jedan proces kriptira podatke, dok ih drugi zaštićuje od neovlaštenih promjena.

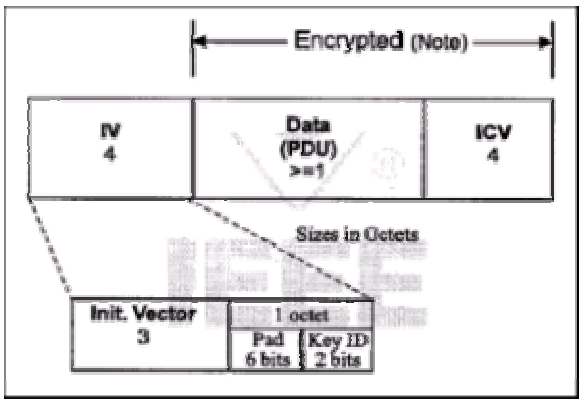
Tajni ključ, duljine 40 bita, se kombinira s inicijalizacijskim vektorom IV, duljine, 24 bita. Ova operacija rezultira 64-bitnim ključem. Taj ključ služi generatoru pseudoslučajnih brojeva (*engl. Pseudo-random Number Generator*, „PRNG“), za generiranje niza slučajnih brojeva koji predstavlja novi ključ baziran na ulaznom ključu. Enkripcija se obavlja XOR operacijom između generiranog niza i ulaznih podataka. Rezultat ovog postupka su enkriptirani okteti koji su po duljini ukupnog paketa jednaki duljini paketa koje treba prenijeti, plus 4 dodatna okteta. Razlog tome je što se ključ koristi također za zaštitu integritetne vrijednosti (*engl. Integrity Check Value*, ICV, 32 bita), a ne samo podataka.

Zaštita od neovlaštene promjene podataka izvodi se na izvornom paketu podataka pomoću integritetnog algoritma (CRC -32), kojim se dobiva ICV.



Slika 3. *WEP dekripcija*

Kod dekripcije, za stvaranje potrebnog ključa, koristi se inicijalizacijski vektor dolazne poruke. Pomoću kriptiranog teksta i ispravnog ključa dobiva se originalan tekst poruke i ICV. Ispravnost poruke provjerava se izvršavanjem integritetnog algoritma na pristigloj poruci, te uspoređivanjem dobivenog ICV' sa pristiglim ICV. Ako oni nisu jednaki, poruka je prenijeta s pogreškom. Procedura WEP dekriptiranja prikazana je na slici 3., dok je format WEP paketa prikazan na slici 4.



Slika 4. *Paket koji se šalje WEP algoritmom*

3.1. Upravljanje ključevima

Standardom 802.11 definirane su dvije metode korištenja WEP ključeva. U prvoj metodi dozvoljeno je korištenje četiri ključa, no sam prijenos podataka ograničen je na samo jedan od njih – standardni (*engl. default*) ključ. U drugoj metodi (*engl Key mapping method*) svaka jedinstvena MAC adresa može imati svoj ključ, a svi oni pohranjeni su u pristupnoj točki (AP).

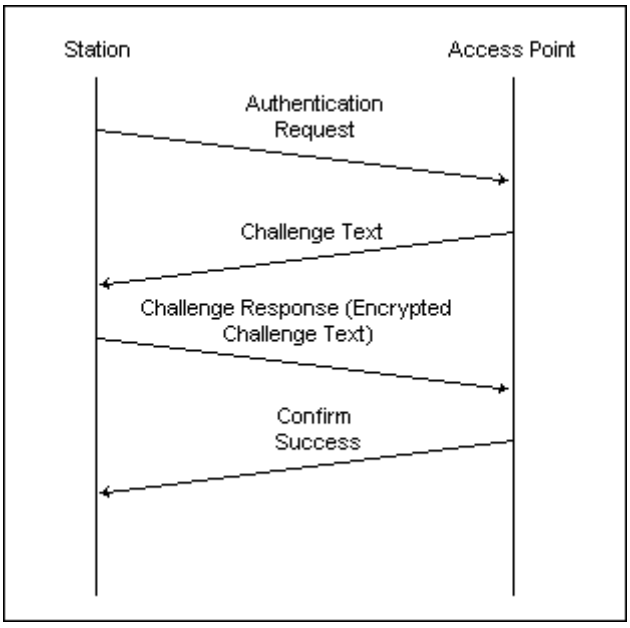
3.2. Autentifikacija

Protokolom 802.11 propisana su dva tipa autentifikacije:

- autentifikacija otvorenog sustava
- autentifikacija temeljena na dijeljenoj tajni (*engl Shared key autentification*)

Autentifikacija otvorenog sustava je nulta autentifikacija. Stanica može komunicirati s bilo kojom pristupnom točkom i *slušati* sve podatke koji se šalju bez enkripcije. Ovaj tip autentifikacije se obično implementira gdje je jednostavnost uporabe bitnija od sigurnosti.

Kod autentifikacija temeljene na dijeljenoj tajni, potrebna je ugradnja WEP-a, a pruža bolju autentifikaciju nego što je slučaj kod otvorenog sustava. Tijek ove autentifikacije prikazan je na slici 5.



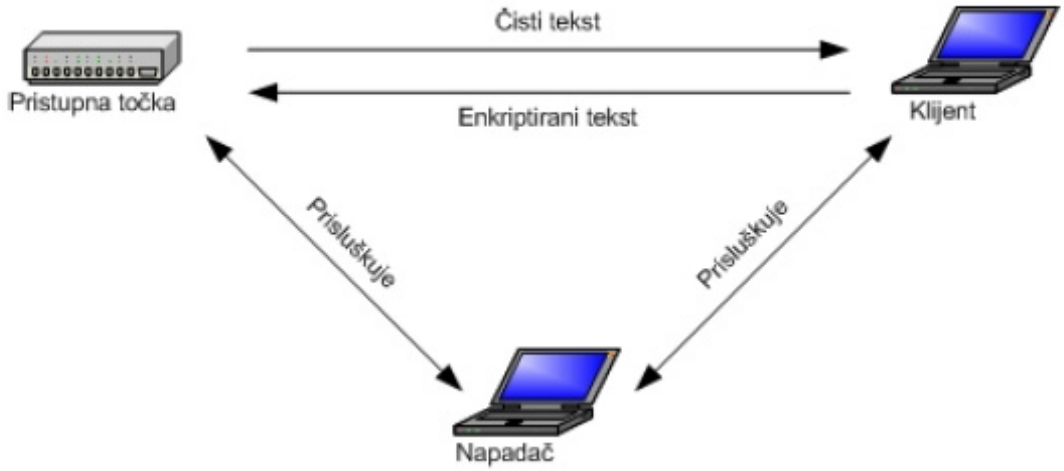
Slika 5. *Autentifikacija temeljena na dijeljenoj tajni*

Tijek autentifikacije:

1. stanica koja zahtijeva autentifikaciju šalje autentifikacijski okvir pristupnoj točci,
2. AP odgovara autentifikacijskim okvirom koji se sastoji od 128 okteta slučajnog teksta generiranog pomoću WEP-a,
3. stanica koja zahtijeva uspostavu veze tada kopira tekst u autentifikacijski okvir, enkriptira dijeljenim ključem, te šalje okvir pristupnoj točci,
4. AP dekriptira tekst koristeći se istim dijeljenim ključem i uspoređuje ga s poslanim tekstom. Ako su tekstovi jednaki, AP će odgovorit uspješnom autentifikacijom. Ako usporedba nije valjana , autentifikacija nije uspješna.

3.2.1. Propusti u autentifikaciji korisnika

Iz upravo opisane procedure vidi se da klijent od pristupne točke dobiva tekst koji treba enkriptirati, te ga poslati natrag. Ovaj način autentifikacije ranjiv je na tzv. napade tipa "čovjek u sredini" (*engl. man-in-the-middle attack*), koji je prikazan na slici 6.



Slika 6. *Napad čovjek u sredini*

Napadač koji prisluškuje može uhvatiti tekst koji je AP poslala klijentu, a zatim i enkriptirani tekst. Pomoću ta dva teksta i IV- a, on može dobiti pristup mreži.

3.3. Propusti WEP algoritma

Okviri poruka su standardnog oblika, te je jednostavno doći do inicijalizacijskog vektora koji je korišten u enkripciji. Provođenjem XOR operacije nad dva enkriptirana bloka moguće je dobiti rezultat jednak onome koji bismo dobili da smo proveli isti postupak nad porukama sa čistim tekstom. Zahvaljujući ovom svojstvu, u slučaju poznavanja jedne čiste riječi, automatski se može doći do druge. Također, veći broj poznatih enkriptiranih riječi, povećava mogućnost otkrivanja podataka. Rješenje ovog problema je česta izmjena tajnog ključa ili inicijalizacijskog vektora.

Polje inicijalizacijskog vektora široko je 24 bita, što znači da je vjerojatnost da će se koristiti za više od jednog okvira vrlo velika. Broj mogućih različitih inicijalizacijskih vektora je 2^{24} = 16 777 216. Uzimajući u obzir da prosječna stanica odašilje okvire veličine 1500 okteta pri propusnosti 5 Mbps, sve mogućnosti će se iscrpiti za manje od pola dana. Standard ne propisuje da se inicijalizacijski vektor treba mijenjati, te su odluke o tome prepuštene proizvođačima. Dva najčešća odabira inicijalizacijskog vektora su:

- slučajni odabir – vjerojatnost da dva okvira imaju isti IV je 50% nakon 4823 odaslana okvira, a 99% nakon 12430 odaslanih okvira
- inkrementiranje nakon svakog odaslanog okvira – vjerojatnost kolizije je 100% nakon što dva uređaja koja se koriste ovom metodom počnu odašiljati okvire

3.4. Napadi na WEP

Napadi koji se provode na WEP algoritam se mogu podijelit na dva osnova tipa:

- Pasivni napadi: Napadač prisluškuje komunikaciju, ali ne utječe na podatke koji se razmjenjuju.
- Aktivni napadi: Napadač aktivno utječe na promet koji se odvija na mreži.

3.4.1. Pasivni napadi

- Analiza prometa

Napad analize prometa je prisluškivanje mreže s namjerom praćenja prometa (broja i veličine podataka) mreže. Potrebe napadača su odgovarajuća antena, mrežna kartica koja radi u modu za slušanje i programska podrška za brojenje i analizu

veličina paketa. Korištenjem ove vrste napada, moguće je saznati količinu prometa na mreži, fizičku lokaciju pristupnih točaka i korištene vrste protokola.

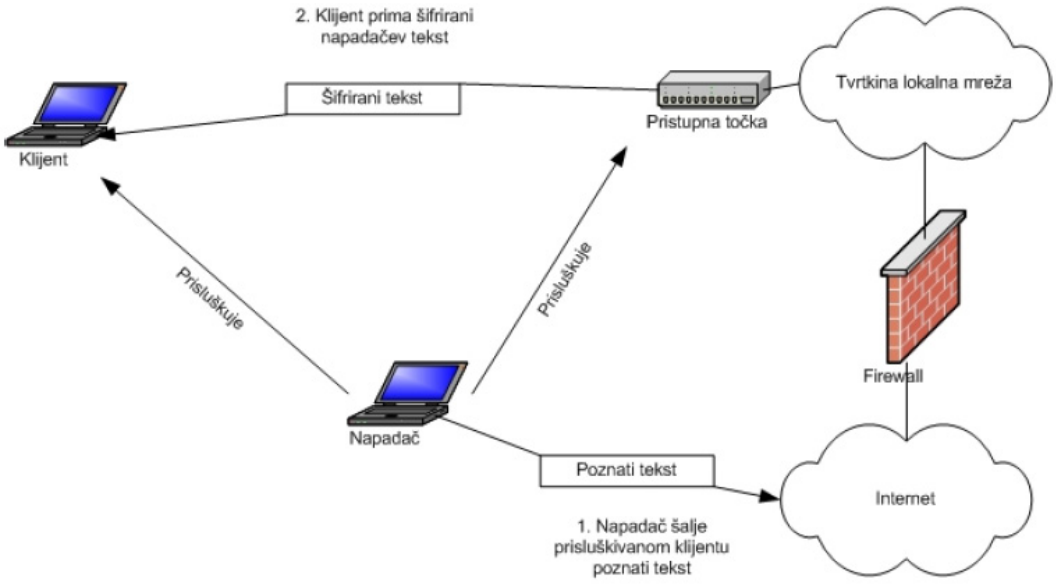
- Pasivno prisluškivanje

Za ovaj napad jedini je uvjet pristup signalu mreže. Kao i prethodno opisani napad, i ovaj se sastoji samo od slušanja prometa mreže. Pri osluškivanju, napadač čeka da se ponovi isti inicijalizacijski vektor, te na ranije opisani način dolazi do podataka. Ako napadač ne poznaje nijednu poruku, uz dobivene informacije o protokolu, može pretpostaviti neke konstantne dijelove poruke te tako doći do podataka.

3.4.2. Aktivni napadi

- Napad ponavljanjem inicijalizacijskog vektora

Napadač šalje poruku klijentu kojega želi napasti, te čeka da AP pošalje tu poruku klijentu. U tom trenutku on ima IV i poznatu poruku te lako može maknuti enkripcijsku zaštitu. Time je u mogućnosti dodavati podatke u enkriptirani paket. Za ovaj napad potrebna je pretpostvaka da se IV i WEP ključ mogu ponavljati dok mreža ne prihvati paket.



- *Slika 7. Napad ponavljanjem IV – a*

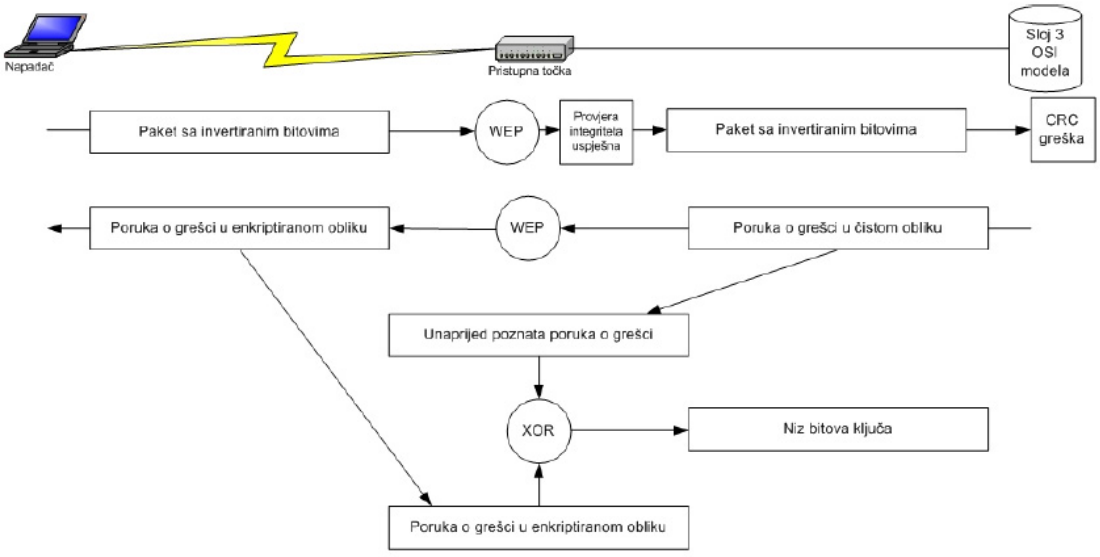
- Napad obrtanjem bitova podataka

Ovaj napad iskorištava slabost ICV-a. Postupak napada je slijedeći:

Napadač prisluškuje mrežu, pokupi jedan okvir te promijeni proizvoljan broj bitova u njemu. Zatim promijeni sadržaj polja u kojem se nalazi ICV, te takav izmijenjeni okvir šalje natrag u mrežu. Prijemna strana računa ICV primljenog paketa te uspoređuje tu vrijednost s dobivenom vrijednošću ICV-a poruke: Ukoliko su ti brojevi jednaki, paket je prihvaćen i predaje se trećem sloju OSI modela. Na tom sloju provjera integriteta ne uspijeva. AP stoga šalje predvidljivi izvještaj o greški, koji napadač očekuje. Nakon što ga prepozna i primi, napadač ima niz bitova ključa.

Postupak mijenjanja ICV-a :

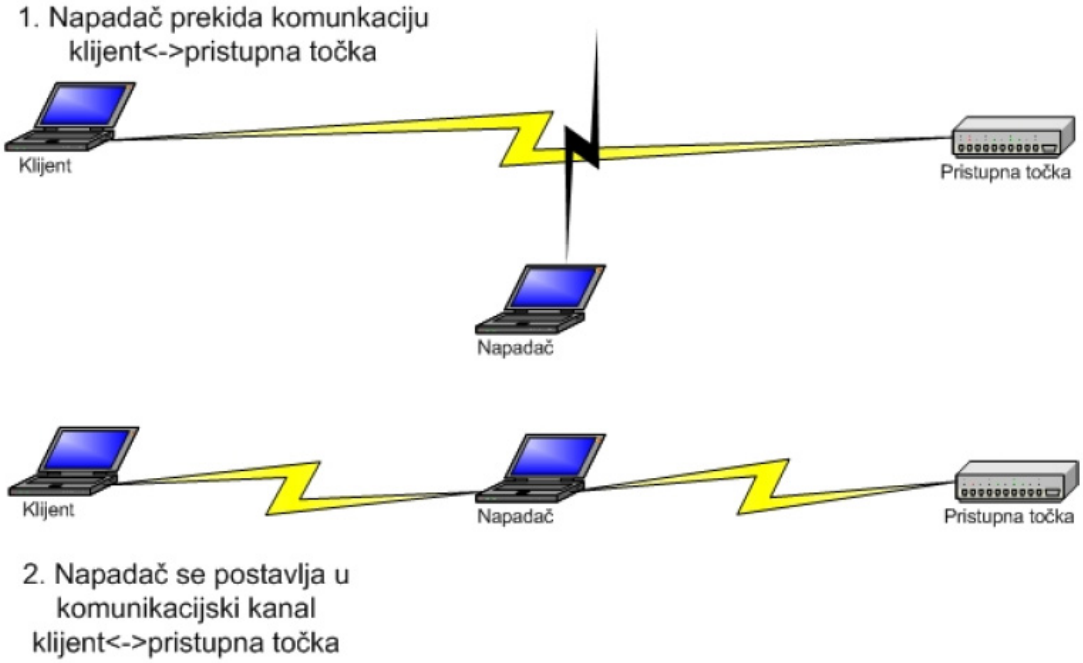
Paket kojem se želi promijeniti ICV je C1. Generira se paket jednake duljine s izmijenjenim bitovima F2. Treći paket se dobije izvršavanjem XOR operacije nad C1 i F2, te time dobivamo F3. Napadač računa ICV za F3 (C2), te se konačni ICV koji će se umetnuti računa pomoću XOR operacije između C1 i C2 vrijednosti. (C3 = C1 XOR C2)



Slika 8. *Napad obrtanjem bitova*

- Napad "čovjek-u-sredini" (*Man-in-the-middle attack*)

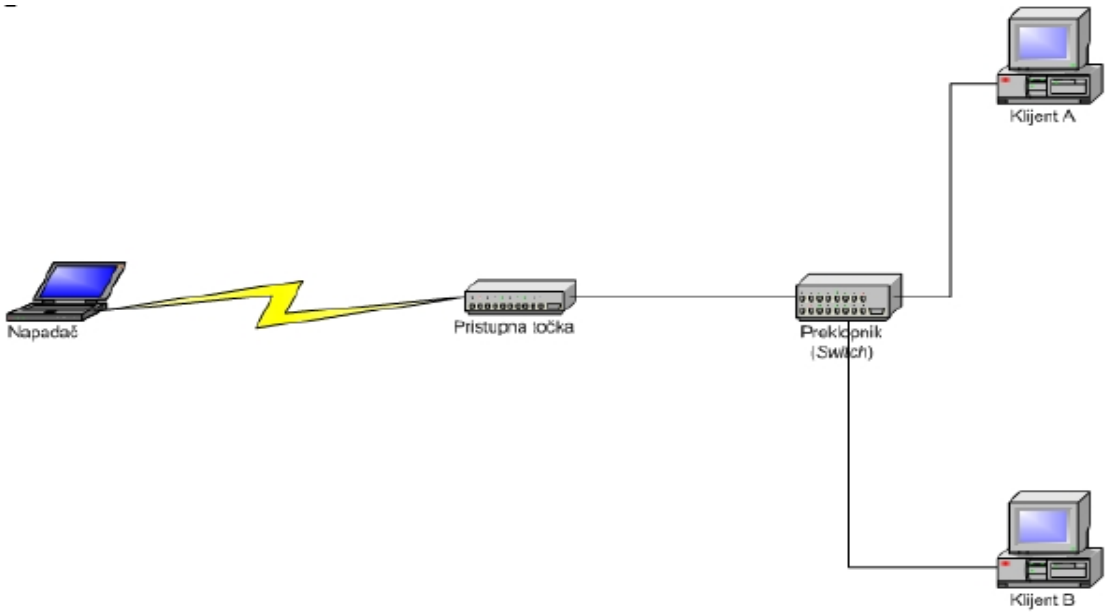
Ovim napadom moguće je čitanje i modificiranje podataka poruke. Napadač se postavlja u komunikacijski kanal između klijenta i pristupne točke i presreće njihovu komunikaciju. Zatim prekida njihovu komunikaciju, te zabranjuje klijentu da ponovo uspostavi komunikaciju. Napadač uspostavlja komunikaciju s klijentom glumeći pristupnu točku. Također je na ovaj način moguće uspostaviti i komunikaciju s pristupnom točkom tako da se napadač predstavi kao klijent.



Slika 9. *Napad čovjek-u-sredini*

- ARP napadi

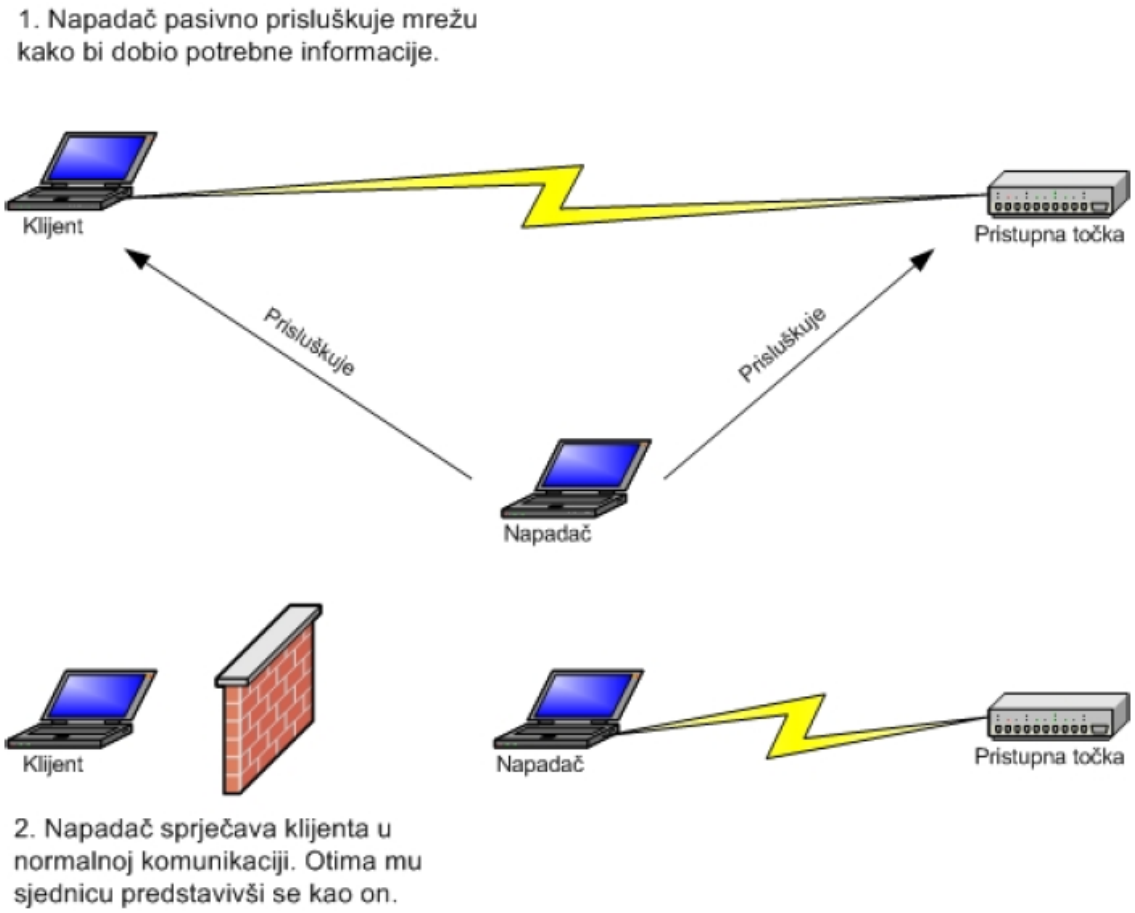
Adress Resolution Protocol (ARP) je protokol koji služi za prevođenje IP adrese koja se koristi u trećem OSI sloju, u fizičku (MAC) adresu koja se koristi u drugom sloju. Za izvedbu ovoga napada potreban je pristup mreži, ali napadač ne mora uspostaviti vezu sa klijentom već se samo krivo predstavlja pristupnoj točci. Napadač šalje krivotvoreni odgovor na ARP upit i time mijenja način na koji su do tada bile povezane IP i MAC adrese klijenta. Sada se on nalazi između pristupne točke i klijenta i može utjecati na njihovu komunikaciju.



Slika 10. *ARP napad*

- Krađa sjednice (Sesion Hi-jacking)

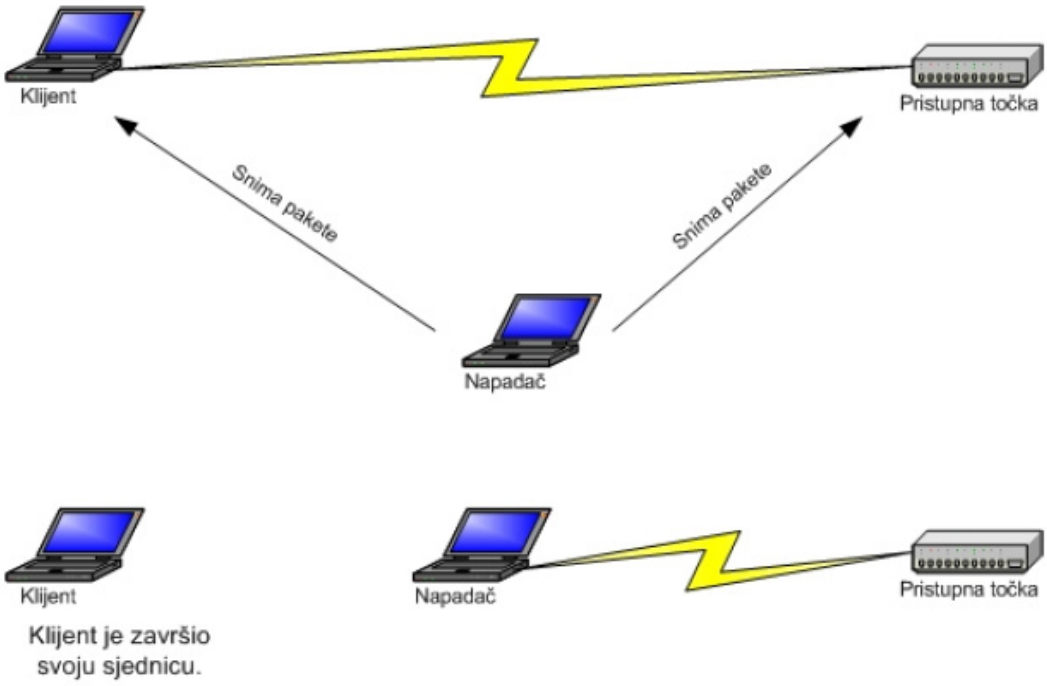
Napadač se prvo mreži mora prikazati kao meta, što se izvršava krivotvorenjem paketa višeg sloja, korištenjem metode autentifikacije koju mreža koristi, te primjenom zaštitne enkripcije u slučaju da je i ona tražena. Napadač zatim šalje lažirane kontrolne okvire koji meti signaliziraju prekid sjednice čime je spriječio komunikaciju mete i pristupne točke. Meta tada zna da je izgubila sjednicu, ali joj to izgleda kao ispad bežične mreže.



***Slika 11**. krađa sjednice*

- Napad ponavljanjem paketa (*Packet re-play attack*)

Ovim napadom napadač dobiva pristup mreži ali ne utječe na sjednice koje su u tijeku. Prvo snima sjednicu između klijenta i pristupne točke, te kada klijent svoju sjednicu završi, ponavlja njegove pakete i time dobiva pristup mreži.



Slika 12. *Napad ponavljanjem paketa*

4. Zaključak

U ovom tekstu prikazali smo osnovne ranjivosti i nedostatke WEP algoritma. Vidimo da njih ima popriličan broj, te da je za sigurnost WLAN-ova potrebno više od korištenja WEP algoritma. Preporučuje se korištenje dodatnih sigurnosnih komponenti, dok proizvođači kao što je CISCO rade na unapređenju i prihvačanju novih standarda koji bi osigurali veći stupanj sigurnosti za bežične mreže.

5. Literatura

1. Overview of IEEE 802.11b Security
   http://developer.intel.com/technology/itj/archive/2000.htm
2. Security of the WEP algorithm
   http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
3. Sigurnost bežičnih računalnih mreža, seminarski rad , Ivica Marić, FER, Zagreb 2004.
4. Sigurnost bežičnih LAN-ova
   http://www.cert.hr/documents.php?cat=6&lang=hr
5. Sigurnost bežičnih LAN mreža
   http://www.cert.hr/documents.php?cat=6&lang=hr