SIGURNOST PODATAKA U Wi-Fi MREŽI U BH KOMPANIJAMA

Prof. dr. Husnija Bibuljica, email: h_bibuljica@hotmail.com
Mr. sc. Haris Bibuljica
Internacionalni univerzitet Travnik u Travniku, Bosna i Hercegovina

Sažetak: *Zaštita podataka u računarskim mrežama je uvijek aktuelna tematika. Zbog pogodnosti koje pružaju bežične računarske mreže se pogotovo naglo šire. Istovremeno u njima je lako dostupan medijum za prenos podataka pa su još izloženije na napade. Iz tih razloga postaje neophodno posvetiti više pažnje njihovoj sigurnosti. Pri implementaciji bežičnih mreža postavlja se pitanje definicije politike sigurnosti, prije svega koju opremu i metode zaštite podataka odabrati. U ovom radu su, kao teoretska osnova, iznijete neke od osnovnih postavki teorije informacija. Navedeni su najčešće korišteni standardi za bežične računarske mreže, a standardi IEEE 802. 11x. i IEEE 802.16 su detaljnije obrađeni. Razmotreni su mehanizmi zaštite podataka i u okviru njih detaljnije analizirane slabosti i prijetnje po sigurnost. Obradio sam i prikaz programa izmjene MAC adrese kao jednog od načina sigurnosti mreže. Prikazane su sistematizovno mjere za poboljšanje sigurnosti podataka u bežičnim računarskim mrežama i detaljnije su opisane neke od tehničkih mjera.*

Ključne riječi: *Sigurnost podataka, WLAN, kriptovanje, kompanije*

DATA SECURITY IN THE WI-Fi NETWORK IN BH COMPANIES

Abstract: *Data security in computer networks are very actual thematic. Accommodation provided by wireless network causes their spiral expansion. In the other hand easy connection to the medium for transmission of data making this networks much exposed to the attacks. Because of that it is necessary to pay much attention about data security in this networks. During the implementation of wireless networks we must decide how to define security policy and as part of this question we must decide what is equipment and data security method best for selection. In this paper as theoretical base are exposed some basic thesis in information theory. There are named often used standards for wireless networks, and standards IEEE 802. 11x. and IEEE 802.16 are detailed presented. There are discussed mechanism for data protection, and in this frame work detailed analyzed weakness and threats for data security. I elaborated the program to change the MAC address of one of the means of network security. Showing systematic measures to improve data security in wireless computer networks and described in more detail some of the technical measures.*

Keywords: *Data security, WLAN, Encryption, Companies*

Uvod

Pogodnosti koje pruža bežična računarska mreža su je učinile popularnom pa se ona danas veoma često koristi. Na primjer, u poslovnom okruženju, univerzitetima, na javnim mjestima, a također i u privatnim kućama. Sigurnost podataka koji se u bežičnim računarskim mrežama prenose je sve češće pitanje koje opredjeljuje korisnike. Medijum za prenos informacija je eter, što znači da bilo ko sa radio prijemnikom i predajnikom može da prima i šalje podatke. To je prijetnja po povjerljivost informacija koje se u takvim mrežama prenose.

U vrijeme kada je WEP prihvaćen, postojala su značajna ograničenja u hardverskim mogućnostima opreme i cijeni njene proizvodnje što je dovelo do prihvatanja ovakvog mehanizma zaštite podataka. WEP se pokazao kao ranjiv na nekoliko vrsta napada i sada sesmatra da ima malu vrijednost kao mehanizam za zaštitu povjerljivosti podataka. U ovom radu je prikazano kako WEP radi i nekoliko načina za probijanje zaštite koju on pruža. Da bi se poboljšala sigurnost, i iskoristila postojeća oprema koja je korištena sa WEP mehanizmom, zaštita je unaprijeđena WPA mehanizmom. To je bilo prelazno rješenje, sa još uvijek nedovoljno efikasnom sigurnošću. Tek WPA2 uz AES i novi sistem autentikacije konačno obezbjeđuje potreban nivo sigurnosti podataka. Aktuelni sistemi zaštite su proizvod ljudskog rada, namijenjen drugim ljudima. Do grešaka u primjeni zaštite podataka najčešće dolazi zbog nerazumijevanja koncepta na kojem se zasnivao razvoj takvih sistema. Da bi se to prevazišlo razvijaju se novi inteligentni sistemi zaštite podataka uz primjenu obsevera i inteligentnog softvera.

1. Informacione mreže i sigurnost podataka

Informacioni sistem je integrisani skup komponenti za sakupljanje, snimanje, čuvanje, obradu i prenošenje informacija. Poslovna preduzeća, druge vrste organizacija i pojedinci u savremenom društvu, zavise od informacionih sistema za upravljanje svojim operacijama i djelovanjima, održavanje kompetitivnosti na tržištu, ponudu različitih usluga i unaprijeđivanje ličnih sposobnosti i kapaciteta. Za primjer, moderne korporacije zavise od računarskih informacionih sistema da bi obrađivale svoje finansijske račune i poslovne transakcije, i upravljale ljudskim resursima; opštinske uprave zavise od informacionih sistema za ponudu osnovnih usluga svojim građanima; pojedinci koriste informacione sisteme da bi unaprijeđivali svoja znanja,za kupovinu, upravljanje bankovnim računima i transakcijama, kao i za različite finansijske operacije.

Uopšteno informacioni sistem se sastoji od izvora informacije, enkodera informacije, komunikacionog (prenosnog) kanala, dekodera i prijeminka informacije.

Slika 1. Opšti prikaz informacionog sistema[169]

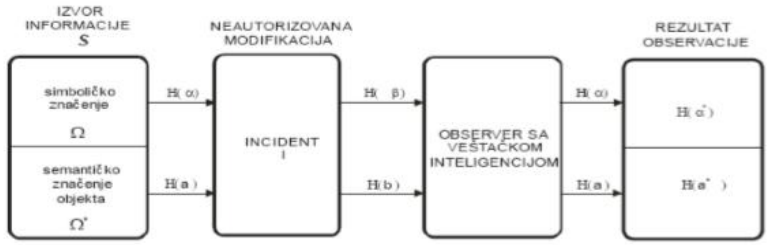
Osnovni servisi sigurnosti su povjerljivost, integritet i dostupnost informacije. Povjerljivost (engl. confidentiality) je jedan od glavnih motiva za uvođenje kriptografskih sistema. Ona znači kontrolu objavljivanja informacija i zaštitu od neovlašćenog pristupa informacijama. Da bi opravdali svoju upotrebu kriptografski sistemi moraju biti efikasni u obezbjeđenju povjerljivosti podataka. Ta efikasnost se naziva snaga: jak kriptografski sistem je teško „razbiti“. Umjesto snage, često se koristi pojam radnog faktora (work factor) algoritma: on približno određuje vrijeme koje je neophodno za „razbijanje“ nekog kriptografskog sistema.

Smatra se da je kriptografski sistem slab ako dozvoljava upotrebu slabih ključeva, ako

[169] Ross Anderson. Security Engineering: A Guide to Building DependableDistributed Systems. Cambridge, January 2011.

posjeduje propuste u dizajnu ili ako se može lako dekriptovati.[170]

Utvrđivanje postojanja eventualnih izmjena poruke tokom prenosa predstavlja drugi osnovni zadatak kriptografskih sistema. Integritet podataka se obezbjeđuje dodavanjem zasebnih podataka u vidu kontrolne sume ili drugih redundantnih podataka koji će biti iskorišteni u procesu dekriptovanja. Dodavanjem koda za autentičnost poruke (engl. Message Authentication Code - MAC) predstavlja uobičajeni način za provjeru njenog integriteta. MAC se dobija na osnovu sadržaja same poruke i ključa. MAC se obično kriptuje sa samom porukom, i tako šalje, čime se dodaje još jedan sloj provjere integriteta. Prijemna strana takođe na identičan način proračunava MAC vrijednost i poredi svoj rezultat sa vrijednošti koja je poslata uz poruku. Integritet je obezbjeđen ukoliko su te dvije vrijednosti iste. Više nije dovoljno da alat bude automatizovan i adaptivan (da bi prebrodio greške korisnika). Alat se mora



ponašati kao inteligentni observer, sposoban da prepozna „nenormalan„ oblik ponašanja informacionog toka. On također mora biti sposoban da donosi neke odluke i da bude u stanju da potpuno rekonstruiše informaciju kakva je bila prije neovlašćenih izmjena.

Slika 2. Napadnuti informacijski sistem sa inteligentnim observerom

2. Planiranje Wi-Fi mreže

Faktore koje treba uzeti u obzir u fazi planiranja su potrebno područje pokrivenosti, kapaciteti i troškovi. U pravilu, neko prostrano područje i veliki kapacitet mogu samo postići visoke cijene. Drugim riječima, manje prijenosno napajanje, manje područje pokrivenosti. S druge strane, to dovodi do većeg ukupnog kapaciteta, tako što se pristupne točke stavljaju bliže jedna drugoj. U kontrolisanim mrežama podešavanje snage je općenito automatsko: prijenos snage je smanjena ako su pristupne točke locirane blizu jedna drugoj.

U smislu kapaciteta, pravilo je da je jedna pristupna tačka se nalazi na oko 10-15 aktivnih korisnika koje mogu poslužiti. Limit za povezivanje, tj. najveći broj korisnika koji se može spojiti na pristupnu točku istovremeno je znatno viši (oko 30-50 korisnika, ovisno o modelu pristupne točke). Stariji modeli pristupne točke, imaju manji kapacitet. U načelu, pokrivenost područja može za planiranje koristit oba 2.4 i 5 GHz širinu frekvencija. U 5 GHz širinifrekvencija se signal gubi jače kao funkcija udaljenosti i kao rezultat prepreka nego u 2,4 GHz. Pokrivenosti područja su gotovo jednaki, međutim, signal jačine od 5 GHz omogućava više snage prijenosa. Međutim, treba naglasiti s obzirom na razlike između frekvencija, da usmjeravanje antene ne mora nužno raditi na 5 GHz.

Postoje najmanje tri načina obavljanja planiranje područja pokrivenosti: ortodoksni i metodičan način, planiranje utemeljeno na testiranje, i planiranje na osnovu zahtjeva korisnika. Međutim, treba napomenuti, da organizacije koje planiraju svoju mrežu nisu prisiljeni dodati pristupne tačke na mjesta kao posljedica korisnika koji se žale na lošu recepciju signala.[171]

Da biste dobili ideju za pristupne točke o pokrivenosti područja, prijenos podataka treba mjeriti na sljedećim mjestima:[172]

1. U neposrednoj blizini pristupne tačke, npr. neposredno ispod nje (tačka A), 2. U neposrednoj blizini pristupne tačke na istom katu, - iza krivine u hodniku (tačka B1) - iza jednog zida relativno blizu pristupne tačke (tačka B2) - iza jednog zida dalje od

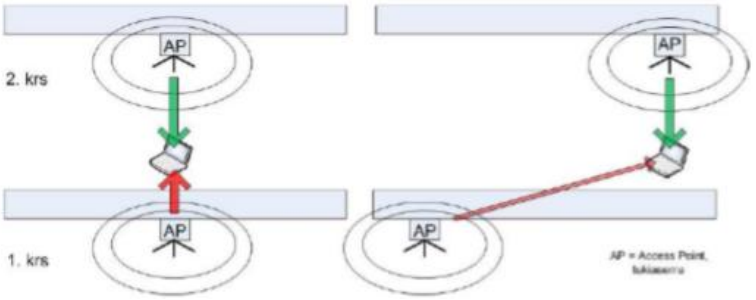
[170] Suzana Stojaković - Čelutska. Building Secure Information Systems, dissertation. Prague. 2000.

[171] http://www.sourceforge.net/projects/iperf/

[172] http://www.sourceforge.net/projects/iperf/

pristupne tačke (tačka B3) 3. Neposredno iznad pristupne tačke na katu iznad (tačka C) ili neposredno ispod pristupne tačke na katu niže (tačka D).

Nakon WLAN testova moguće je procijeniti koliko često pristupne tačke trebaju biti raspoređene za pokrivanje velikog područje (s obzirom na željenu brzina prijenosa podataka). Željena brzina prijenosa podataka može odrediti samostalna, dajući dužnu pozornosti na željene ukupne pokrivenosti područja i proračun. Međutim, rezultati ispod 10 Mbps ne bi smjeli biti u fazi planiranja. Međutim, treba napomenuti, da stvarni rejtinzi podataka mogu u najgorem slučaju ostati ispod toga. Ništa ne sprječava kontroler-based pristupnih tačaka od toga, ako proračun dopušta.U praksi, mjestu Ethernet i utičnice, a u starim zgradama, vidljivost pristupne tačke, također je potrebno uzeti u obzir pri postavljanju pristupnih tačaka. Gdje je



moguće, pristupne tačke bi trebale biti smještene sustavno dok ne bude cijela zgrada pokrivena. Međutim, sljedeći faktori moraju se uzeti u obzir kako bi se osigurala najmanje moguća smetnje između pristupnih tačaka: Zidovi i podovi / plafoni spriječivaju pristup područja pokrivenosti tačke od toga da bude potpuno sferična.

Slika 3. Smetnje između pristupnih tačaka.[173]

Ako se pristupne tačke stavljaju neposredno iznad ili ispod svake druge, njihovi signali će se međusobno ometati (lijevo). Ako su pristupne tačke koje se nalazi u nešto različitim mjestima na različite etaže, ometani signal slabi dok putuje kroz strop, što je rezultiralo manje smetnje (desno).Ukupni plan mreže omogućuje mrežu kako bi se trebala postaviti, potencijalni problemi mogu se riješiti nakon optimizacije mreže.

3. Softverski alati za analizu bežičnih mreža

Kismet je alat otvorenog koda (open source).[174]
Prvenstveno je namijenjen za detekciju pristupnih tačaka i prikupljanje raznih informacija o pristupnim tačkama. To su informacije poput identifikatora mreže, jačine signala, zaštite koja se koristi, pa čak i informacije o klijentima koji su spojeni na dotičnu pristupnu tačku. Kismet također čuva dosta podataka u dnevničkim datotekama (engl. log files) što ga čini vrlo atraktivnim. Za razliku od nekih drugih alata, Kismet ne samo da detektuje pristupne tačke, već bilježi kompletni zapis svih uhvaćenih paketa. Takvi zapisi mogu se naknadno iskoristiti pomoću drugih alata (Ethereal, Wireshark) za dalju analizu.

Korisna informacija, koju također možemo dobiti pomoću Kismet, alata je popis klijenata koji su spojeni na pristupnu tačku.U pogledu liste klijenata dostupna je informacija o MAC adresi svakog klijenta, a u određenim slučajevima također je moguće dobiti informaciju o tipu kartice koju dotični klijent koristi. Identifikuje se i broj paketa koje je Kismet uhvatio i broj paketa koji su kriptovani. Kismet ima i mogućnost identifikovanja IP adrese klijenata i snage njihovog signala.

4. Probijanje zaštite bežičnih mreža

Još od vremena kada se pojavio poznati rad na temu kako krekovati WEP ključ postoji dosta radova na temu slabosti i propusti u WEP mehanizmu zaštite sigurnosti podataka. Kao zamjenu za WEP korisnici su

[173] http://www.smallnetbuilder.com/content/view/30224/100/

[174] http://www.kismetwireless.net/

prihvatili najpre VPN i 802.1X. Takvo rešenje je dozvoljavalo korištenje postojeće mrežne opreme uz poboljšanje sigurnosti podataka. Zatim je uslijedilo privremeno rješenje u vidu WPA mehanizma. WPA je otklonio većinu poznatih sigurnosnih propusta uočenih kod WEP. Sa poboljšanjem sigurnosti raste i složenost podešavanja sigurnosnih mehanizama, a to opet uzrokuje da primjena u praksi bude manja nego što se očekuje. Konačna zamjena za WEP i WPA je WPA2 (IEEE 802.11i) za koji do sada u varijanti enterprise nema objavljenih slabosti po pitanju sigurnosti. Praktični primjeri u ovom poglavlju su izvršavani pod Linux operativnim sistemom zbog ograničenog broja bežičnih mrežnih adaptera koji imaju potrebne funkcionalnosti. Većina navedenih primjera bi se mogla izvršti i pod Windows platformom.

5. Mjere za poboljšanje sigurnosti WLAN-a

Upravljačke mjere za zaštitu bežičnih mreža

Upravljačke mjere za zaštitu sigurnosti počinju sa obuhvatnom politikom sigurnosti. Politika sigurnosti je dokument na osnovu kojeg su ostale mjeresigurnosti, operativne i tehničke usklađene i implementirane. Sigurnost bežične mreže uključuje sljedeće odrednice:[175]
Ovlaštenja i odgovornosti korisnika - Politika prikazuje šta je sve u nju uključeno, zašto je ona neophodna i šta se dešava ako se ona prekrši. Ona također definiše odgovornost službi i pojedinaca, posebno korisnika uopšte, odeljenja IT i kontrolora. Sredstva koja se štite - Politika sigurnosti može identifikovati ili ukazati na osjetljive informacione resurse, komunikacione kanale i sisteme koje treba zaštiti u bežičnoj mreži. Prijetnje i slabosti - Politika sigurnosti može da uključi i dio u kojem se identifikuju prijetnje po bežičnu mrežu. Analiza napada - Politika sigurnosti može identifikovati posljedice koje nastanu u slučaju narušavanja sigurnosti bežične mreže. Postupci i odgovornosti - Politika sigurnosti bi trebalo da identifikuje i definiše sigurnosne procedure za sljedeće slučajeve: Planiranje odgovora na narušavanje sigurnosti Operativne mjere za zaštitu sigurnosti bežičnih mreža Fizička sigurnost je osnovna mjera kojom se obezbjeđuje da samo autorizovani korisnici imaju pristup bežičnoj računarskoj opremi. Fizička sigurnost podrazumijeva mjere kao što su: Kontrola pristupa - Identifikacija propusnicama, pristup uz identifikaciju putem čitača kartica, identifikacija biometrijskim uređajima su metode koje smanjuju mogućnost neovlaštenog pristupa opremi za bežičnu računarsku mrežu. Lična identifikacija. Zaštita na više nivoa - zaključavanje vrata, instalacija video nadzora za nadgledanje prostora oko objekata u kojima je postavljena WLAN. Na taj način se odvraćaju potencijalni napadači na pristupne tačke.

6. Zaključak

Bežične računarske mreže su sigurnosni rizik za svakoga ko ih koristi. Uzroke treba tražiti u nepotpunoj primjeni postojećih mehanizama zaštite kao i u još uvjek važećim standardima 802.11a, 802.11b i 802.11g koji kao osnovu sigurnosti koriste WEP.

Prvi rezultat toga je i donošenje 802.1X standarda koji znatno poboljšava način autentifikacije korisnika i time povećava ukupnu sigurnost. Taj standard kao svoju osnovu koristi EAP koji omogućava veliki broj različitih metoda autentifikacije korisnika mreže. Sljedeći korak u evoluciji sigurnosti je WPA standard koji je usvojen od strane udruženja proizvođača mrežne opreme za bežične računarske mreže (Wi-Fi Alliance). WPA je otklonio sve sigurnosne propuste u WEP-u, a pri tome uz manje promjene drajvera radi na postojećoj opremi. Iako veliko poboljšanje WPA se smatra samo međukorakom između 802.11x standarda i najnovijeg 802.11i standarda koji se nameće kao konačno rješenje problema sigurnosti bežičnih računarskih mreža.

Kada govorimo o zaštiti firme trebamo obratiti pažnju još na par dodatnih stvari

[175] Robbie Gill. Security Note on WPA and WPA2 dictionary attacks. 2008.

radi bolje sigurnosti bežične mreže. Firme su i potencijalno zanimljivije hakerima, jer u firmu uvijek postoji makar jedan „nemaran“ uposlenik čije greške hakeri mogu doći do povjerljivih podataka o firmi, budućim projektima il pak bankovnim računima. Treba obratiti pažnju na sam pristup signalu, treba ga ograničiti u granicama radnog okruženja, to je moguće preko softvera regulacijom i usmjerenjem antene, ali i fizičkoj izolaciji signala na krajnjim zidovima te firme. Osim kontrole pristupa lokalnom odašiljaču, jednaka opasnost vreba i od „prisluškivanja“. Naime, kontrolom korisnika koji pristupa lokalnom odašiljaču, nismo onemogućili trećoj osobi unutar dometa lokalnog odašiljača da prisluškuje komunikaciju između odašiljača i prijemnika (našeg računala) i na taj se način potencijalno domogne osjetljivih podataka (npr. lozinki za internet bankarstvo i sl.).

Literatura

[1] Diskusioni forum: http://www.netstumbler.org. 02.2009.
[2] Hall var Helleseth. Data set of WEP encrypted frames. 02 2007.
[3] http://www.sourceforge.net/projects/iperf/
[4] http://www.smallnetbuilder.com/content/view/30224/100/
[5] http://www.kismetwireless.net/
[6] http://www.elitesecurity.org/f24-Kriptografija-enkripcija
[7] http://www.willhackforsushi.com/Cowpatty.html . 05.06.2009.
[8] http://www.tamos.com/. 05.06.2009.
[9] IEEE lista proizvođača opreme i OUI kodova. http://standards.ieee.org/regauth/oui/. 16.02.2009.
[10] Itisk Martin Scott Fluhrer i Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. http://www.crypto.com.papers/others/rc4.ksaproc.pdf.
[11] Martin Beck, Erik Tews. Practical attack against WEP and WPA. 2008.
[12] Matthew Gast: 802.11 Wireless Networks: The Definitive Guide, O'Reilly, 2002.eBooks
[13] M. Barbeau. WiMax/802.16 Threat Analysis. ACM Press. str. 8-15, 2005.
[14] Robbie Gill. Security Note on WPA and WPA2 dictionary attacks. 2008.
[15] Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Cambridge, January 2011.
[16] Suzana Stojaković - Čelutska. Building Secure Information Systems, dissertation. Prague. 2000.
[17] Thomas Maufer. Field Guide to Wireless LANs for Administrators and Power Users. Prentice Hall PTR. 2003.
[18] William A. Arbaugh. Real 802.11 Security. 2001.