HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost bežičnih LAN mreža

CCERT-PUBDOC-2003-03-06

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Popularnost bežičnih LAN mreža sve više i više raste zbog svoje jednostavnosti implementacije te gotovo neograničenim mogućnostima pristupa. Zbog tih značajki bežična LAN rješenja zadnjih godina primijenjena su unutar mnogih organizacija.

Iako bežične LAN mreže posjeduju razne sigurnosne elemente, iznenađuje činjenica da velik broj organizacija uopće ne koristi nikakve mehanizme koji bi osigurali bilo kakvu razinu sigurnosti. Pokazuje se da prilikom uspostave bežičnih rješenja uvijek treba uzeti u obzir implikacije vezane uz upravljanje i sigurnost.

Čak i ukoliko se aktiviraju sigurnosni mehanizmi definirani IEEE 802.11 standardom, to ne znači nužno da je postignuta zadovoljavajuća razina sigurnosti. Statički WEP (engl. *Wired Equivalent Privacy*) standard koji se koristi za uspostavu sigurnosti u sebi sadrži mnoge sigurnosne nedostatke koji su naknadno otkriveni.

Jedini način osiguranja prihvatljive razine sigurnosti na takvim mrežama bila bi dodatna implementacija VPN tehnologija, zajedno sa svim troškovima.

Čak je i Cisco priznao nedostatke u statičkom 802.11 WEP standardu, te je ponudio unaprijeđeno Cisco Aironet bežično LAN rješenje. Korištenjem sigurnosnih elemenata definiranih kroz IEEE 802.1x standarde za 802.11 mreže, Cisco Aironet osigurava dinamičku sigurnost definiranu na razini korisnika i razini sjednice. Na taj način eliminirani su mnogi nedostaci statičkog WEP standarda, te je unaprijeđena sigurnost.

Sigurnosne značajke uključuju mehanizme koji osiguravaju obostranu autentikaciju, sigurno generiranje i razmjenu ključeva, dinamičke WEP ključeve, politike za ponovnu autentikaciju, te promjene vezane uz inicijalizacijski vektor (IV).

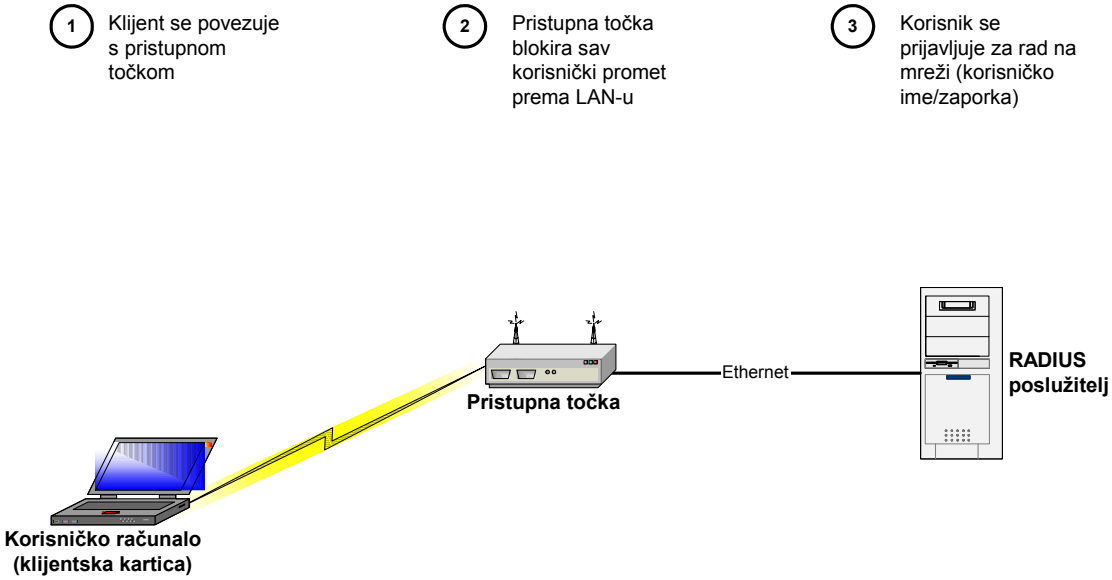
2. Sigurnosni mehanizmi

2.1. Obostrana autentikacija

Mnoga trenutno raspoloživa rješenja koriste jednostavne mehanizme jednostrane autentikacije. Korištenje takvih mehanizama omogućava razne mogućnosti tzv. *man-in-the-middle* napada, gdje napadač može presresti komunikaciju npr. korištenjem svojih pristupnih točaka (engl. *access points*), te na taj način prikupljati povjerljive informacije sa klijenata, kopirati ili mijenjati pakete, te ih ponovno vraćati u mrežu kao valjane.

Važno je naglasiti da pri korištenju bežičnih rješenja nikako ne valja koristiti pretpostavke prilikom uspostave komunikacije. Uvijek valja osigurati autentikaciju obje strane, klijenta i pristupne točke koja pruža pristup mrežnim resursima. Obostrana autentikacija je pri tome jedino prihvatljivo rješenje kojima se mogu izbjeći ranije spomenuti napadi.

U Aironetu Cisco je predstavio autentikacijsku shemu temeljenu na EAP (engl. *Extented Authentication Protocol*) protokolu, koja je poznata kao EAP-Cisco Wireless ili LEAP. Kao temelj se koristi 802.1x standard za sigurnost temeljenu na razini porta, sa nužnim promjenama za uporabu u bežičnim mrežama. LEAP osigurava obostranu autentikaciju između Cisco Aironet klijentskih kartica i pozadinskog RADIUS poslužitelja (Slika 1).



Slika 1: *RADIUS autentikacija unutar Cisco Aironet bežičnih mreža*

2.2. Autentikacija i sigurno generiranje ključeva

Prva generacija 802.11 proizvoda koristila je statičke WEP ključeve za autentikaciju i šifriranje, te je na taj način potencijalno činila sustav ranjivim na tzv. *password-reply* napade. Aironet sustav razdvaja autentikaciju i šifriranje. Tijekom obostrane autentikacije, korištenjem zajedničkog tajnog ključa konstruiraju se individualni odgovori na *challenge* upite. Ti odgovori se šifriraju korištenjem jednosmjernih *hash* vrijednosti originalnog zajedničkog tajnog ključa. Ovaj mehanizam, zajedno sa dobrim odabirom zaporki i njihovog mijenjanja osigurava otpornost na napade primjenom čiste sile (engl. *brute-force*).

Jednokratni sjednički ključ generira se korištenjem MD5 *hash* vrijednosti zajedničkog tajnog ključa i međusobno izmijenjenih tzv. *challenge-response* poruka. Ova metoda sprječava napadača da generira sjednički ključ presretanjem samo odgovora na *challenge* upite. Sigurnost se temelji na nemogućnosti inverzije jednosmjerne funkcije. Također, korištenje slučajnih *challenge* upita osigurava da se sjednički ključ mijenja nakon svake ponovne autentikacije.

2.3. Dinamički WEP ključ

IEEE 802.11 standard prepustio je implementaciju WEP shema za upravljanje ključevima proizvođačima. Većina 802.11 proizvoda prve generacije koristila je jedan, zajednički ključ za sve korisnike na mreži. Taj pristup u sebi je sadržavao mnoge probleme, od kojih je najočitiji rizik od izgubljenog ili ukradenog uređaja koji sadrži ključ.

Drugi problem bilo je upravljanje WEP ključevima. Zajednički ključevi koji se koriste za statički WEP moraju se ručno unijeti u svaku pristupnu točku, isto kao i u svaki klijentski uređaj, što može biti postupak koji zahtijeva mnoge resurse, pogotovo u slučaju kada sigurnosna politika zahtijeva čestu promjenu ključeva. Taj nedostatak ovaj mehanizam čini gotovo neupotrebljivim u većim mrežnim okruženjima. Za takve sustave jedino rješenje je uporaba dinamičkih ključeva.

2.4. Ponovna autentikacija

Veliki nedostatak bežičnih LAN mreža jest njihova otvorenost za napade umetanjem prometa, kod kojih napadači koriste predvidljive uzorke da bi umetnuli svoje pakete u mrežu. Iako 802.11 WEP standard predviđa obranu od napada umetanjem prometa i statističkih napada, statičke WEP implementacije ne primjenjuju te obrane na ispravan način.

Šifriranjem toka podataka, kratki ključ se proširuje na beskonačni, pseudoslučajni ključ. Pošiljatelj korištenjem tog ključa provodi XOR operaciju nad otvorenim podacima da bi dobio šifrirane podatke. Primatelj koristi isti ključ da bi dobio identični pseudoslučajni ključ, te mogao dešifrirati šifrirane podatke. Napadač može iskoristiti ovaj nedostatak presretanjem prometa, te izmjenom bitova i umetanjem tako modificiranih paketa nazad u mrežu. Ukoliko napadač presretne dva šifrirana podatka sa istim pseudoslučajnim ključem i inicijalizacijskim vektorom, korištenjem statističkog napada može doći i do originalnih podataka.
Aironet 802.1x eliminira mogućnost statističkih napada promjenom vrijednosti inicijalizacijskog vektora na razini paketa, tako da napadači ne mogu pronaći predodređeni niz. Također, sjednice započinju sa slučajnim vrijednostima inicijalizacijskog vektora, što u sprezi sa ponovnom autentikacijom, te promjenom inicijalizacijskih vektora otežava mogućnost provođenja sličnih napada.

2.5. Korištenje CRC-32 kontrolnih suma

Provjera integriteta je također jedna od značajki 802.11 standarda koja je ranjiva, pošto originalno koristi linearne CRC-32 kontrolne sume, što napadačima omogućava računanje razlike između dvije CRC sume koje nastaju promjenom bitova u poruci. Niti jedan od standarda, 802.1x, niti 802.11 ne dotiču ovo pitanje.
Napadač može promijeniti paket i CRC na odgovarajući način, tako da paket bude legitiman. Jedini način eliminiranja ovog nedostatka je provjera integriteta poruke na razini paketa, koju treba implementirati u budućim proizvodima.

2.6. Interoperabilnost

Nekoliko kompanija, uključujući pri tom Cisco, Microsoft i još neke kompanije, radi zajednički na razvoju interoperabilnog sigurnog okvira za bežične LAN mreže. Temeljen na standardima poput EAP-a ili RADIUS-a, 802.1x za 802.11 osigurava skalabilni okvir koji omogućava razne autentikacijske sheme koje uključuju uporabu biometrijskih podataka, digitalnih uvjerenja i jednokratnih zaporki.
Zahtjevi koji su nužni u bežičnim okruženjima, kao što su, između ostalog, obostrana autentikacija i zaštita od napada ponavljanjem, zahtijevaju unaprjeđenje autentikacijskih shema korištenih u tradicionalnim okruženjima poput standardnih ožičenih ili *dial-up* mreža.

3. Zaključak

Osiguranje bežičnih LAN mreža je samo jedna od komponenti nužnih za osiguranje sigurnosti unutar organizacije. Stručnjaci predlažu implementaciju nekoliko razina obrane na mreži da bi se izbjegle sve prijetnje. Također, predlaže se uporaba dodatnih sigurnosnih komponenti kao što su IDS sustavi, vatrozidi, te segmentirane računalne mreže.
Ciscova implementacija 802.1x bežične sigurnosti predstavlja unaprjeđenje u odnosu na statički WEP standard, te u mnogome poboljšava sigurnost. Aironet sustavi štite bežična okruženja od mnogih napada, dok Cisco i drugi proizvođači rade na unaprjeđenju i prihvaćanju novih standarda koji bi eliminirali i preostale poznate sigurnosne nedostatke.
U ovom slučaju brzina je od ključnog značaja pošto je sloboda bežičnih IP mreža korištenjem prijenosnih i PDA računala vrlo privlačna i osigurava brzo širenje tih tehnologija.