SECURITATEA ÎN REȚELELE *WIRELESS* BAZATE PE STANDARDUL 802.11. PROBLEME ȘI SOLUȚII. EVOLUȚII ALE STANDARDULUI 802.11 ÎN MATERIE DE SECURITATE

Drnd. ing. Mocanu Ştefan

Universitatea Politehnica *Bucureşti*
smocanu@rdslink.ro

Rezumat: Articolul de față prezintă un aspect deosebit de important al comunicațiilor fără fir și anume, securitatea oferită de rețelele wireless, bazate pe standarde din familia IEEE 802.11. În prima parte, sunt descrise metodele implicite, de asigurare a securității oferite de standardul 802.11, problemele care pot să apară din folosirea exclusivă a acestor metode și câteva măsuri de contracarare a acelor probleme. În cea de a doua, parte sunt prezentate standardele 802.1X și 802.11i, ambele reprezentând evoluții ale standardului 802.11 în sensul oferirii unei mai bune securități.

Cuvinte cheie: 802.11, WLAN, protocoale, securitate, probleme de securitate, filtrarea adreselor MAC, WEP, SSID, algoritmul RC4, EAP, TKIP.

1. Introducere

Dezvoltarea într-un ritm alert a rețelelor *wireless* a venit pe fondul creșterii accentuate a numărului de echipamente mobile de calcul și a aplicațiilor care presupun o mobilitate ridicată a utilizatorilor. Necesitatea interconectării facile și rapide a echipamentelor și rularea în aceleași condiții a aplicațiilor au determinat o serie de organisme internaționale și companii din domeniul comunicațiilor și tehnicii de calcul să facă demersurile necesare realizării unor noi standarde. Dintre inițiativele finalizate, se remarcă: standardul **802.11** elaborat de IEEE; standardul **Bluetooth** dezvoltat de IBM, Intel, Ericsson, Nokia și Toshiba; **HiperLan** dezvoltat de ETSI (European Telecommunications Standards Institute - Institutul European pentru Standarde în Telecomunicații) [amănunte despre aceste standarde precum și alte asemănătoare pot fi găsite în 7].

Standardul **802.11** acoperă aspecte legate de nivelul fizic și de nivelul de control al accesului la mediu (MAC)[1], [4], [6]. Nivelul fizic se referă la transmisia/recepția datelor între stații. Nivelul MAC gestionează accesul la mediu, având în sarcină și securitatea transmisiilor. În plus, oferă facilități precum [8]:

- protecție împotriva stațiilor ascunse,
- fragmentare,
- roaming,
- autentificare și comunicare privată.

Pe baza standardului **802.11** pot fi construite două tipuri de rețele *wireless* [4,6]:

- rețea ad-hoc: cel mai simplu tip de rețea; devine operativă de îndată ce două dispozitive *wireless* se află suficient de aproape pentru a se stabili o conexiune între ele;
- rețea bazată pe infrastructură: în acest model, unul sau mai multe puncte de acces (Access Point – AP) joacă rol de intermediar între un client și o rețea cablată.

Pe baza standardului **802.11**, au fost realizate câteva variante, toate acestea formând ceea ce am numit deja „familia de standarde 802.11". Pot fi incluse aici: 802.11a (802.11 la 5 GHz), 802.11b (sau 802.11 HR), 802.11g, 802.1X și 802.11i. Primele trei au avut ca obiectiv principal creșterea vitezei de transmitere a datelor. Ultimele două - abordează problema stringentă a asigurării unui nivel înalt de securitate în rețelele *wireless*.

2. Securitatea implicită a standardului 802.11 și problemele inerente

Spre deosebire de rețelele LAN cablate, comunicația în rețelele *wireless* se bazează pe un mediu liber, care este imposibil de controlat. Din acest motiv, este evident pentru oricine faptul că o rețea WLAN este mult mai puțin sigură decât o rețea LAN cablată. Una din cele mai mari probleme ale rețelelor WLAN constă în faptul că undele radio sunt foarte ușor de interceptat, fără ca acest lucru să fie depistabil. Mai mult decât atât, oricine posedă o dotare tehnică minimală poate emite unde radio. Iată de ce securitatea într-o rețea WLAN trebuie să acopere ambele aspecte.

Standardul **802.11**, în varianta sa de bază, oferă 3 metode de securizare a rețelelor WLAN:

- SSID (Service Set Identifier);
- filtrarea adreselor MAC (MAC address filtering);
- WEP (Wired Equivalent Protocol).

2.1. Securitatea bazată pe SSID

Acest identificator poate fi folosit pentru a selecta clienții cărora li se va acorda permisiunea de a accesa rețeaua. Fiecare AP poate fi configurat cu un anumit SSID, specific unui anumit WLAN. Atunci când un calculator-client dorește să acceseze rețeaua, acesta trebuie să aibă același SSID, în caz contrar, nu va fi acceptat de către AP. Metoda este relativ rudimentară, și nu oferă o securitate foarte bună. Standardul **802.11** prevede posibilitatea configurării AP-urilor astfel încât acestea să își facă cunoscut SSID-ul. Cu alte cuvinte, un AP transmite un semnal de tip baliză, semnal care este recepționat de către toți clienții aflați în aria de acoperire a AP-ului și din care aceștia află SSID-ul pe care trebuie să îl folosească dacă doresc să acceseze rețeaua. Cu opțiunea de transmitere a SSID activată în AP, rețeaua devine publică, practic, nu mai există nici o barieră împotriva accesului unor clienți nedoriți. Din acest motiv, în cazul rețelelor care nu se doresc publice, se recomandă dezactivarea opțiunii de transmitere a SSID.

O altă problemă legată de SSID provine din faptul că nu este protejat împotriva furtului fizic. Un potențial client rău-voitor ar putea obține SSID-ul specific rețelei de la un client valid, dacă are acces la calculatorul acestuia. Există câteva soluții și recomandări și pentru această situație. În primul rând, accesul la resursele calculatorului trebuie sever restricționat mai ales când este vorba despre configurările acestuia. O restricționare severă se poate realiza prin reluarea autentificării, de fiecare dată când utilizatorul/administratorul dorește să acceseze și/sau să modifice anumite configurări ale sistemului. În acest fel, se poate evita situația în care utilizatorul, deja autentificat, este nevoit să plece de lângă calculator pentru o perioadă scurtă de timp, lăsând, astfel, posibilitatea unui intrus să obțină informații critice.

De departe cea mai bună metodă de asigurare a confidențialității SSID constă în a limita accesul la configurarea SSID-ului atât pe calculatoarele-client, cât și pe AP. Conform principiului că un secret este cel mai bine protejat atunci când nu îl comunici și altei persoane, administratorul rețelei va fi singurul în măsură să aibă acces la configurarea SSID. Din păcate, clienții unei rețele WLAN sunt reprezentați, în cea mai mare măsură, de calculatoare portabile, astfel încât această metodă ar fi extrem de neconvenabilă pentru administrator.

2.2. Securitatea bazată pe filtrarea adreselor MAC

Această metodă se bazează în totalitate pe presupunerea că adresa MAC a fiecărei plăci de rețea este unică. Plecând de la această presupunere, se pot imagina diverse metode prin care AP să refuze accesul unui client nedorit. Cea mai simplă dintre acestea ar fi construirea unei liste cu adrese MAC valide, pe care AP-ul să o parcurgă de fiecare dată când primește o cerere din partea unui client [3]. Dacă adresa MAC a clientului nu se află în lista predefinită din AP, accesul la rețea nu îi va fi a acordat. Cel mai mare inconvenient al acestei metode îl reprezintă timpul de căutare în listă, timp care poate fi considerabil în cazul unor AP-uri cu clienți numeroși. Se recomandă folosirea acestei metode numai în cazul în care numărul de clienți ai unui AP este redus și alături de metoda bazată pe SSID.

Furtul adresei MAC reprezintă, ca și furtul SSID, o altă mare problemă în securizarea unui WLAN. Așa cum spuneam încă de la început, metoda filtrării adreselor MAC se bazează pe unicitatea acestor adrese, ceea ce se reflectă în identificarea precisă a clienților de către AP și la respingerea clienților nedoriți. Din păcate, standardul **802.11** nu prevede o protecție a adresei MAC, astfel că un atacator care a intrat în posesia unei adrese MAC valide o poate folosi pentru a lansa cereri de acces la rețea [10]. Din punctul de vedere al AP-ului, nu se poate face distincția între clientul real și cel fals, ambii folosesc aceeași adresă MAC, deci, ambilor li se va permite accesul în rețea. Singura barieră pe care o poate ridica AP-ul este aceea de a nu permite accesul simultan a doi sau mai mulți clienți cu aceeași adresă MAC.

2.3. Securitatea bazată pe WEP

WEP, în traducere liberă „protocolul echivalent celui din rețele cablate", a fost adoptat de IEEE, în urma eforturilor de a înlătura problemele de securitate ale WLAN. Cu toate că WEP nu și-a atins în totalitate scopurile propuse, acesta oferă o securitate mai bună decât SSID și Filtrarea adreselor MAC. În cele ce urmează, vor fi descrise caracteristicile WEP, problemele de securitate ce apar, precum și câteva metode de combatere a problemelor de securitate.

WEP se bazează pe bine-cunoscutul algoritm de criptare RC4 [9], ceea ce înseamnă că toți clienții și AP-urile dintr-o rețea *wireless* vor folosi o cheie pentru criptarea și decriptarea datelor, în timpul comunicației. Pe calculatoarele-client va exista o cheie secretă, în timp ce AP-ul va avea o cheie publică [11] folosită la criptare. Din păcate, standardul **802.11** nu prevede un protocol de management al acestor chei, ceea ce înseamnă că ele trebuie gestionate manual. Acest fapt are un impact negativ asupra securității WLAN întrucât, din comoditate,

cheile pot rămâne neschimbate pentru o perioadă mare de timp. Astfel, un client care a avut cândva acces la rețea și apoi a devenit nedorit, va putea, totuși, să intre în rețea folosind vechea cheie [11]. Din acest motiv, se recomandă cu tărie schimbarea cât mai frecventă atât a cheii publice, cât și a cheii private, chiar dacă presupune un anumit disconfort pentru utilizatorii care vor fi nevoiți, astfel, să își reconfigureze toate dispozitivele de rețea. O soluție mult mai elegantă ar fi implementarea unui mecanism dinamic de generare a cheilor.

Pentru a evita criptarea a două pachete de date cu aceeași cheie și pentru a reduce riscul ca un atacator să ghicească o cheie secretă, WEP prevede posibilitatea folosirii unui vector de inițializare (VI). Pornind de la cheia publică (cu care se criptează primul pachet de date), VI se folosește la generarea de noi chei pentru criptarea tuturor pachetelor din timpul comunicației. Mecanismul de decriptare este similar, însă, trebuie făcută o precizare. Pentru a putea genera toate cheile de decriptare, este necesar de știut vectorul de inițializare, folosit la criptare. Din acest motiv, apare necesitatea transmiterii în clar a acestuia, fapt care se realizează prin includerea sa într-o parte necriptată a pachetului. Din păcate, schimbarea VI cu fiecare pachet transmis este doar o recomandare, și nu o cerință impusă de WEP. Prin urmare, implementări de WLAN-uri la care se folosește o singură cheie pentru toate pachetele transmise pot fi întâlnite în practică, fără a fi ne-conforme cu standardul **802.11**.

Managementul slab al VI, pentru care WEP rezervă un câmp de numai 24 biți, aduce după sine alte probleme de securitate [11]. Un studiu efectuat asupra unui AP mediu-solicitat relevă o probabilitate crescută de repetare a VI după transmiterea a numai 5000 de pachete, ceea ce se rezumă la un interval de timp de numai câteva ore. Din acest motiv, cheia de criptare poate fi descoperită și întâmplător, fără ca un potențial hacker să mai folosească metode sistematice de căutare. Din păcate, lungimea insuficientă, rezervată pentru IV, nu poate fi corectată fără a se compromite conformitatea cu standardul **802.11**.

În plus, față de problema legată de VI menționată anterior, există încă un aspect negativ, care ar trebui luat în considerare de producătorii de plăci de rețea *wireless*. Cele mai numeroase dispozitive care accesează o rețea *wireless* sunt, de departe, calculatoarele portabile. În cazul acestora, dimensiunea redusă impune o folosire la maximum a spațiului disponibil și folosirea alternativă a unor dispozitive. Este și cazul plăcilor de rețea de tip PCMCI care se introduc în calculatorul portabil numai atunci când se dorește conectarea la rețea. Problema acestor plăci este aceea că, în general, oferă minimul necesar pentru a fi conforme cu standardul **802.11**. Întrucât nu există nici un fel de management pe placă, de fiecare dată când aceasta este introdusă în calculator, vectorul de inițializare este readus la 0 și incrementat cu fiecare pachet transmis. Acest fapt conduce la o reutilizare a valorilor mici ale VI, de vreme ce conectarea/deconectarea plăcilor PCMCI este o operațiune frecventă. Cunoscând VI-ul, un atacator poate afla cheia folosită pentru criptare și, dacă este în posesia unui mesaj criptat cu aceeași cheie, va fi capabil să decripteze toate mesajele ce urmează. Problema poate fi corectată fie prin adăugarea unui modul de management al VI, fie prin adăugarea unui EPROM care să memoreze ultima valoare luată de VI, înaintea deconectării.

Algoritmul RC4 a fost ales drept algoritm de criptare/decriptare datorită performanțelor sale, deși se cunoșteau slăbiciunile sale în materie de securitate. Varianta inițială a implementării s-a bazat pe o cheie de 40 de biți. Această versiune poate fi ușor spartă cu ajutorul calculatoarelor moderne. În practică, s-a constatat o probabilitate de repetare a cheii secrete după aproximativ 16 milioane de mesaje transmise, cu toate că, teoretic, probabilitatea de repetare ar fi trebuit să fie nulă. Eficiența algoritmului RC4 poate fi mult mărită prin folosirea unei chei de 104 biți [11], care este imposibil de spart, cel puțin cu tehnica de la ora actuală.

Un alt rol important al WEP este acela de a garanta integritatea mesajelor transmise printr-o rețea *wireless*. Protocolul WEP trebuie să protejeze atât conținutul, cât și destinația mesajului, ceea ce înseamnă că mesajul transmis de expeditor trebuie să ajungă numai la destinatarul dorit și fără a suferi modificări în timpul transportului. Din păcate, WEP își arată slăbiciunile și în acest caz, mecanismul de securitate folosit nefiind foarte eficient [10]. În fapt, WEP folosește un simplu câmp de verificare a integrității (eng. Integrity Check Field, ICF) pe care îl include în pachet. Acest câmp conține o sumă de verificare, implementată sub o formă binecunoscută: CRC (Cyclic Redundancy Check). Trebuie subliniat faptul că acest CRC [9] este conceput pentru a detecta erori datorate transmisiei, și nu oferă o protecție reală în cazul unor atacuri serioase. Din acest motiv, se recomandă o criptare suplimentară a mesajelor, înainte de transmiterea acestora prin rețea. Acest lucru este ușor de realizat cu ajutorul unei aplicații software de criptare/decriptare, aflată atât pe calculatorul expeditorului, cât și pe calculatorul destinatarului. Cheia de criptare va fi cunoscută numai de către cele două părți, și nu va fi transmisă sub nici o formă prin rețea, ceea ce duce la probabilitatea 0 ca o persoană neautorizată să descifreze un mesaj ce nu îi este adresat.

Ca o concluzie a celor arătate până acum, putem spune că, pentru toate problemele de securitate al standardului **802.11**, se pot găsi soluții relativ simple. Marea provocare constă în a realiza rețele *wireless* foarte sigure și care să fie conforme cu standardul **802.11**. Dintr-un alt unghi de vedere a lucrurilor, cu cât gradul de securitate crește, cu atât rețeaua devine mai dificil de administrat și utilizat. Acest fapt poate avea un impact

negativ asupra utilizatorului mediu, dar acesta trebuie să înțeleagă faptul că o mai bună securitate a rețelei este mai importantă decât comoditatea.

Problemele de securitate ale standardului **802.11** preocupă, în continuare, grupul de lucru IEEE 802.11. Rețelele *wireless* sunt încă la început de drum, astfel că multe din problemele identificate astăzi erau imposibil de anticipat cu nu mult timp în urmă. De asemenea, multe din soluțiile oferite acum se pot dovedi, într-un viitor apropiat, mult mai puțin viabile decât se crede. Cu toate acestea, dezvoltarea standardului **802.11** este un proces continuu, care a dus la elaborarea unor standarde îmbunătățite cum ar fi 802.1x și 802.11i, standarde ce vor fi prezentate în paragrafele următoare. Au fost dezvoltate și soluții proprietar, dar acestea nu sunt foarte răspândite. Cele mai multe dintre ele nu sunt conforme cu standardul **802.11** și, de aceea, nu vor fi subiectul unor discuții în această lucrare.

3. Evoluții ale standardului IEEE 802.11

Pornind de la problemele de securitate, expuse în secțiunea anterioară, și nu numai, comitetul 802.11 a decis modificarea standardului existent și transformarea acestuia într-unul mult îmbunătățit. Ca urmare a acestei acțiuni, în a doua jumătate a anului 2003, va fi lansat un nou standard sub numele de 802.11i. Rezultate parțiale au fost deja lansate sub forma standardului intermediar 802.1X și sunt deja implementate de producătorii de dispozitive *wireless*.

3.1. Standardul 802.1X

Acest standard interimar aduce două noutăți care pot contribui activ la îmbunătățirea securității unui WLAN. Cele două aspecte remarcabile sunt: autentificare securizată și un mecanism de management al cheilor. Criptarea nu a fost abordată în acest standard.

Nucleul standardului **802.1X** este reprezentat de protocolul EAP (engl. Extensible Authentification Protocol). Acesta permite alegerea unui protocol de autentificare, singura condiție fiind ca atât clientul, cât și AP-ul, să folosească același protocol. Dacă această condiție nu este îndeplinită, comunicația nu este posibilă. Există un număr de patru protocoale de autentificare din care se poate face alegerea, în funcție de necesitățile aplicației:

- MD5: oferă autentificare unidirecțională pe baza unei parole;
- Cisco Lightweight Authentication Extension Protocol (LEAP): protocol dezvoltat de CISCO, oferă autentificare bazată pe nume și parolă;
- EAP – Transport Layer Security (TLS): oferă autentificare atât a clientului, cât și a AP-ului, pe bază de certificate;
- EAP-Tunneled TLS (TTLS) și Protected EAP (PEAP): protocoale bazate pe TLS, dar nu necesită certificate la nivelul clientului.

MD5 este cel mai simplu, dar și cel mai slab protocol de autentificare, motiv pentru care nu se recomandă folosirea sa în cazul rețelelor *wireless*. Parolele nu sunt păstrate pe serverul de autentificare, într-o manieră sigură. De fapt, serverul accesează parolele dintr-un fișier text, sub forma unor șiruri de caractere în clar, ceea ce ușurează foarte mult munca unui potențial atacator. Această problemă de securitate se datorează faptului că MD5 autentifică numai utilizatorul, nu și serverul de autentificare, considerat ca fiind sigur. O îmbunătățire notabilă a acestui protocol s-ar putea realiza prin autentificarea ambelor părți.

Cisco LEAP este o soluție de tip proprietar, dezvoltată de CISCO. Oferă o mai bună securitate decât MD5, dar este mai scump de implementat. În plus, este și mai puțin eficient decât alte soluții oferite de standard.

EAP TLS, EAP TTLS și PEAP sunt cele mai bune metode de autentificare și reprezintă prima opțiune atunci când se implementează un WLAN 802.1X. Toate oferă autentificare reciprocă client-AP [10] și chei generate dinamic pe calculatorul-client.

O procedură de autentificare tipică [9] și conformă cu standardul 802.1X implică trei părți: clientul, AP și un server de autentificare. Cel mai adesea, serverul de autentificare este un server RADIUS (enlg. Remote Authentification Dial-In User Service) [5]. AP primește de la un client o cerere de autentificare pe un anumit port și transmite această cerere serverului de autentificare. Până când clientul este verificat și autentificat, AP blochează celelalte cereri de trafic, sosite din partea clientului (de ex. HTTP, POP3, SMTP), astfel că acesta nu are nici o posibilitate de a accesa rețeaua sau resursele acesteia. Dacă autentificarea s-a făcut cu succes, AP îi trimite clientului o cheie de criptare și îi permite accesul la rețea. Procedura de autentificare nu depinde de un anumit protocol de autentificare și este ilustrată în figura 1, pașii descriși mai sus fiind sugestiv marcați.

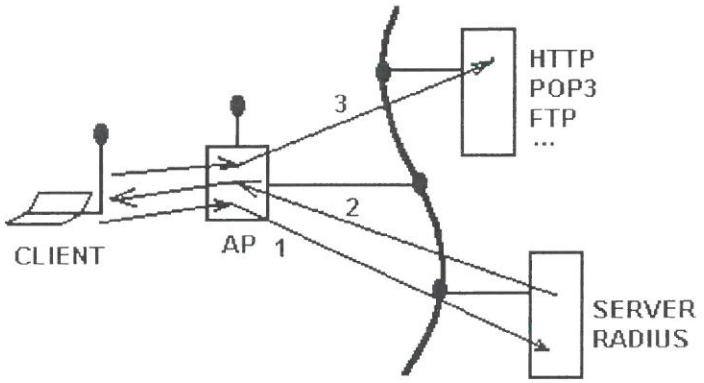

Figura 1. Sesiune de autentificare tipică 802.1X

Managementul cheilor, apărut pentru prima dată în standardul **802.1X**, permite nu numai chei de autentificare pe sesiune, dar oferă suport pentru generarea dinamică a cheilor, în timpul aceleiaşi sesiuni. În acest fel, se îmbunătăţeşte dramatic securitatea unui WLAN. Chiar dacă un atacator reuşeşte să descopere o cheie şi să o folosească la decriptarea unuia sau mai multor pachete interceptate, va fi imposibil să descopere toate cheile folosite la criptarea întregului mesaj, astfel încât să-l poată decripta în totalitate. Cheile sunt generate aleator, spre deosebire de WEP unde se porneşte de la o cheie de bază, şi se generează chei cu ajutorul vectorului de iniţializare, prin incrementare după trimiterea fiecărui pachet. Un nivel şi mai ridicat de securitate poate fi obţinut prin folosirea cheilor generate aleator, pentru fiecare pachet [10], şi reducerea dimensiunii pachetelor. Acest lucru conduce la un număr mai mare de pachete pentru acelaşi mesaj şi, implicit, la creşterea numărului de chei folosite, dar metoda are ca efect negativ creşterea fragmentării şi scăderea vitezei de comunicaţie. În concluzie, metoda este indicată, mai ales, pentru aplicaţiile la care securitatea este mult mai importantă decât viteza.

3.2. Standardul 802.11i

802.11i este ultimul standard IEEE, pentru reţele *wireless*. După cum am precizat la începutul paragrafului, standardul este încă în lucru, varianta sa finală fiind aşteptată în partea a doua a anului 2003. **802.11i** are ca principal obiectiv asigurarea unei bune securităţi în WLAN-uri, aducând o mai bună protecţie datelor şi un control mai bun al clienţilor care accesează reţeaua.

În noiembrie 2002, un subset al standardului **802.11i** a fost lansat de Wi-Fi Alliance [2] (Alianţa Wi-Fi), sub numele de WPA (Wi-Fi Protected Access). Iniţiativa nu a avut ca scop lansarea unui standard interimar, cum este cazul lui **802.1X**, ci numai a acelor componente din standardul final **802.11i**, care s-au dovedit stabile şi care se pot implementa printr-o simplă operaţiune de upgrade a echipamentelor deja existente. În plus, s-a dorit înlăturarea cât mai rapidă a problemelor de securitate ale WEP.

Versiunea finală a standardului **802.11i** vizează securitatea atât a reţelelor ad-hoc, cât şi a celor bazate pe infrastructură, în vreme ce WPA face referire numai la reţelele bazate pe infrastructură. Dintre componentele standardului **802.11i**, se fac remarcate următoarele: mecanismul de autentificare, folosit în 802.1X [5], protocolul de asigurare a integrităţii cheii temporale (engl. Temporal Key Integrity Protocol, TKIP) [12], ierarhizarea şi managementul cheilor, negocierea autentificării şi a algoritmilor de criptare. Alături de noile componente introduse în standard, au fost făcute şi modificări la cele existente în standardul 802.11 de bază. În privinţa WEP, cea mai notabilă constă în înlocuirea algoritmului RC4 cu Standardul de Criptare Avansată (engl. Advanced Encryption Standard, AES).

TKIP permite generarea dinamică a cheilor şi schimbul acestora între clienţi şi AP, ceea ce oferă o mai bună securitate decât cheia statică, folosită de WEP. În prima versiune a TKIP, s-a folosit o variantă pe 128 biţi a algoritmului RC4 pentru a genera chei care se schimbă automat, după un număr de 10000 de pachete trasmise prin reţea. În cazul WEP, problemele generate de CRC au fost remediate prin înlocuirea ICF cu un mecanism de verificare a integrităţii mesajului (enlg. Message Integrity Check, MIC) pentru a preveni modificări aduse în timpul transportului. De asemenea, managementul defectuos al VI din WEP a fost corectat prin introducerea unui VI pe 48 biţi şi prin faptul că acesta nu mai este transmis necriptat prin reţea. Cu toate că este mult mai sigur decât WEP, TKIP este vulnerabil la atacuri datorită folosirii algoritmului de criptare RC4. Acest

compromis a fost făcut pentru a permite implementarea imediată pe hardware-ul existent, dar, în varianta finală a **802.11i**, algoritmul RC4 va fi înlocuit cu AES [5].

Singura problemă a standardului **802.11i**, care poate fi deja anticipată, este creată de incompatibilitatea cu alte standarde, excepție făcând WPA. Din această cauză, nu numai software-ul va trebui înlocuit, ci și echipamentul hardware, ceea ce presupune costuri de implementare ridicate.

4. Concluzii

Fără îndoială, securitatea rețelelor *wireless* va fi mult mai bună din punctul de vedere al standardelor. Totuși, un rol major îl vor avea, în continuare, administratorii de rețea, care au sarcina de a configura cât mai bine atât software-ul, cât și hardware-ul sistemului.

Am arătat în lucrarea de față cele mai mari probleme privind securitatea rețelelor *wireless*, bazate pe standardul IEEE 802.11, și am indicat, acolo unde a fost posibil, soluții la aceste probleme. Este evident pentru oricine că o rețea *wireless* 802.11 este mult mai puțin decât o rețea cablată, dar o administrare corectă și eficientă poate reduce din diferențe. Având în vedere că majoritatea echipamentelor de la ora actuală sunt conforme cu standardul 802.11, la implementarea unui WLAN trebuie ținut cont de următoarele recomandări:

- rețeaua nu trebuie considerată sigură nici dacă, din punct de vedere geografic, este amplasată într-o zonă sigură. Undele radio nu pot fi oprite la o distanță dorită, deci, pot părăsi zona în cauză, permițând, astfel, interceptarea lor;
- toate opțiunile de securitate de pe AP și client trebuie activate;
- confidențialitatea comunicațiilor poate fi îmbunătățită prin folosirea unor măsuri suplimentare de criptare/decriptare;
- combinarea tuturor măsurilor de securitate (SSID, filtrarea adreselor MAC și WEP) în cazul 802.11 este binevenită;
- introducerea unui management al cheilor este, de asemenea, binevenită.

Dacă măsurile luate se dovedesc insuficiente, trebuie luate în considerare si evoluțiile standardului 802.11, chiar dacă implementarea acestora presupune o creștere considerabilă a costurilor.

Bibliografie

1. * * *: IEEE 802.11 and 802.11b Technology, documentație Internet
2. * * *: Pagina Web a Wi-Fi Alliance, http://www.weca.net/OpenSection/index.asp
3. **ARBAUGH, W.A., N. SHANKAR, Y.C.J. WAN**: Your 802.11 Wireless Network has No Clothes, Univ. Maryland , documentație Internet, www.cs.umd.edu/~waa/wireless.pdf
4. **BRENNER, P.**: A Technical Tutorial on the IEEE 802.11 Protocol, documentație Internet, www.sss-mag.com/pdf/802_11tut.pdf
5. * * *: DELL Co. – Wireless security in 802.11 (Wi-Fi®) networks, White papers 2003, documentație Internet.
6. **LOUGH, D.L., T.K. BLANKENSHIP, K. J. KRIZMAN**: A Short Tutorial on Wireless LANs and IEEE 802.11, Institutul Politehnic Bradley – Virginia.
7. **MOCANU, ȘT.**: Transmiterea datelor pe canale wireless, referat doctorat 2002, AII-215-03.
8. **MOCANU, ȘT.**: Evoluția Standardizării în Comunicații Wireless. În: Revista Română de Informatică și Automatică, vol. 13, nr. 1, 2003, pp. 39-45.
9. **SCHAFER, G.**: Network Security & IEEE 802.11 Wireless LANs, Tutorial, Paris, 2002.
10. **SIMON, D., B. ABOBA, T. MOORE**: IEEE 802.11 Security and 802.1X, doc IEEE 802.11 00/034rl, 2000.
11. **WALKER, J.**: Unsafe at any Key Size: an Analysis of the WEP Encapsulation, doc IEEE 00-362, 2000.
12. **WALKER, J.**: 802.11 Security Series, Intel Corporation, documentație firmă, 2002.