MANAGEMENTUL SECURITĂȚII INFORMATICE ÎN REȚELELE FĂRĂ FIR

Mr.ing. Daniel SORA

DEPARTAMENTUL REGIONAL DE STUDII PENTRU MANAGEMENTUL RESURSELOR DE APĂRARE

Abstract

Wireless cellular technology has made the cellular phone a must-have accessory that enables us to instantly communicate with friends, relatives, and business associates. Similarly, computers can also be free of wired connections when they are part of a wireless local area network (LAN) network. However, with this increased freedom comes increased risk of information compromise, particularly in wireless LANs.

This paper explains wireless LAN technologies and addresses the associated wireless network security vulnerabilities and safeguards.

1. Noțiuni introductive.

Familia de standarde pentru rețele fără fir IEEE 802.11 descrie o interfață între un client fără fir şi o stație de bază sau punct de acces, sau între două dispozitive mobile fără fir (wireless). Standardele 802.11 descriu parametrii ambelor nivele ale rețelei: nivelul fizic (PHY) şi nivelul de control al accesului la mediul de comunicație (MAC).

Nivelul PHY este responsabil cu transmiterea datelor între noduri. Familia de standarde suportă rate de transfer cuprinse între 2 Mbps şi 54 Mbps, dar există şi un proiect de nou standard care suporta rate de transfer de 100 Mbps, standardul 802.11n.

Nivelul MAC reprezintă un set de protocoale responsabile cu menținerea ordinii în utilizarea în comun a mediului de transmisie. Standardul 802.11 specifică un protocol de acces multiplu la purtătoare cu evitarea coliziunilor (CSMA/CA) pentru rețelele fără fir. Acest nivel oferă următoarele servicii:

- **Transfer de date** – accesul la mediul de transport CSMA/CA;
- **Asocierea** – stabilirea legăturilor fără fir între clienții fără fir şi punctele de acces din infrastructura rețelei;
- **Reasocierea** – acțiunea care apare ca o consecință a asocierii atunci când un client fără fir se mută de la un **s**et de **s**ervicii de **b**ază (BSS) la altul. Un set de servicii de bază (BSS) este un grup de stații compatibile standardului 802.11 care constituie o rețea fără fir complet conectată.
- **Autentificarea** – procesul care furnizează identitatea clientului prin folosirea mecanismelor specifice standardului 802.11.
- **Confidențialitatea** – în familia de standarde 802.11 există opțiuni pentru diferite nivele de protecție a datelor transmise, care vor fi prezentate mai în detaliu în acest articol.

Standardele 802.11 permit două moduri de lucru: *ad-hoc* şi *infrastructură* (fig. 1).

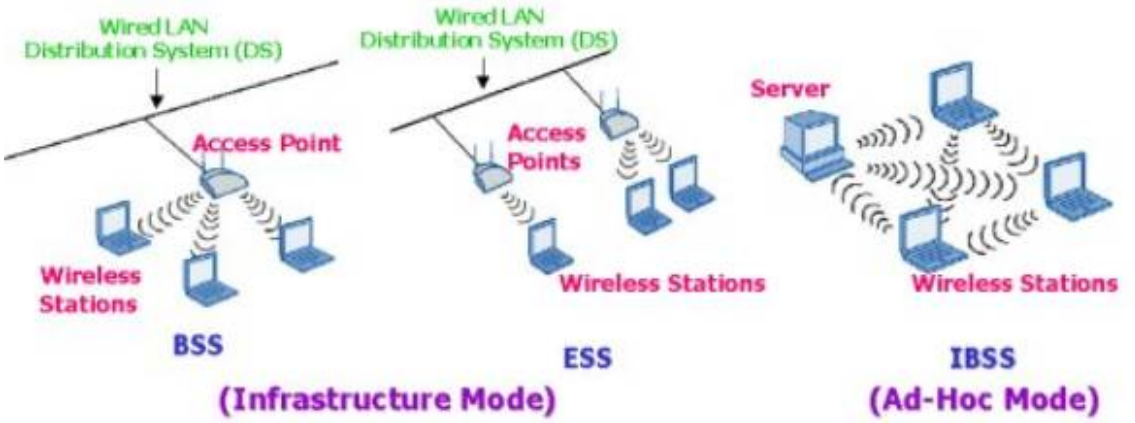

Fig.1

Modul *ad-hoc* se referă la rețele independente (IBSS), compuse din cel puțin două stații fără fir. Acest mod nu se utilizează pe distanțe mari, ci doar în încăperi sau secțiuni ale clădirilor, fiecare client fără fir comunicând punct-la-punct cu ceilalți clienți fără fir din rețea, numai în cadrul aceleiaşi celule. Modul *infrastructură* se referă la rețele care includ puncte de acces pentru comunicarea între dispozitivele mobile şi rețele cu fir, sau cu alte rețele fără fir.

2. Securitatea informațiilor conform standardului 802.11.

Specificațiile originale ale standardului 802.11 definesc o opțiune de securitate, numită Wired Equivalent Privacy (WEP). În conformitate cu aceasta, se configurează o cheie comună pentru comunicarea între punctul de acces şi clientul său fără fir. În standardul 802.11, modul implicit de transfer

al datelor este în clar. Atunci când se doreşte confidenţialitate, opţiunea WEP criptează datele înainte de a fi transmise. Algoritmul utilizat este bazat pe criptarea simetrică RC4, şi presupune existenţe unei chei secrete utilizată în comun de staţia mobilă şi de punctul de acces pentru a proteja confidenţialitatea informaţiilor transmise în reţea. Pachetelor transmise criptat cu cheia secretă li se ataşează un câmp de verificare a integrităţii (IC), bazat pe o sumă de control CRC-32. Implementarea WEP este slabă atât pentru autentificare cât şi pentru confidenţialitate, astfel că poate fi uşor spartă cu programe disponibile pe internet, apărând astfel necesitatea unor sisteme de securitate mai puternice pentru reţelele fără fir.

Cheia simetrică WEP este compusă dintr-o parte variabilă de 24 biţi – Vectorul de Iniţializare (IV) şi o parte fixă – cheia secretă de 40 sau 104 biţi. Întrucât cheia secretă este schimbată rar, scopul vectorului de iniţializare este de a preveni criptanaliza cerându-i clientului să folosească diferiţi vectori de iniţializare pentru criptarea mesajelor (fig.2).

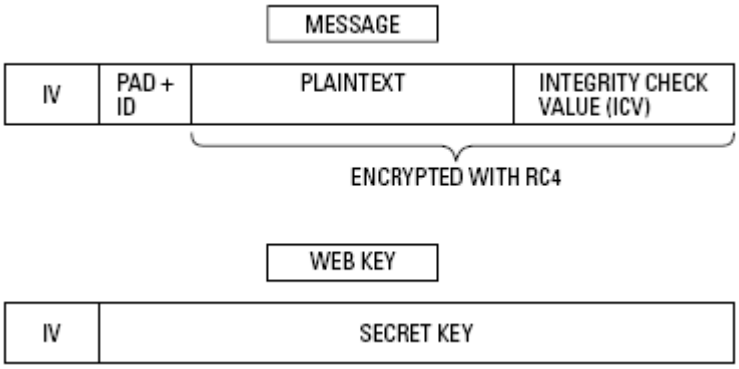

Fig. 2

Se observă că vectorul de iniţializare IV este transmis în clar în pachet. Atunci când punctul de acces primeşte pachetul, funcţia implementată hardware concatenează IV cu cheia secretă cunoscută obţinând astfel cheia utilizată pentru decriptarea pachetului. Întrucât vectorul de iniţializare este scurt, atacatorii pot monitoriza pachetele şi pot descoperi cheile slabe ale WEP, implementând un atac cu un text clar cunoscut. De asemenea, WEP este vulnerabil şi la atacurile de tip imitare şi răspuns, prin care un atacator poate modifica şi retransmite pachetele, sau le poate captura şi transmite ulterior nemodificate.

Autentificarea WEP poate fi deschisă sau pe bază de cheie simetrică comună. În cazul autentificării deschise, clientul transmite un cod numit *Service Set Identity* (SSID), comun tuturor staţiilor din acelaşi segment de reţea, deservite de acelaşi punct de acces. Vulnerabilitatea acestei metode constă în faptul că punctul de acces transmite în clar SSID la anumite intervale, în cadrul cadrelor de management, fiind astfel disponibil atacatorilor pentru a stabili o conexiune cu punctul de acces. Autentificarea cu cheie simetrică comună presupune parcurgerea următorilor paşi:

- Staţia client transmite o cerere de autentificare;

- Punctul de acces răspunde cu o întrebare în clar;
- Clientul alege un IV, cu care, împreună cu cheia secretă cunoscută, criptează întrebarea;
- Clientul transmite IV şi întrebarea criptată către punctul de acces;
- Punctul de acces criptează aceeaşi întrebare folosind IV recepționat şi cheia secretă cunoscută;
- Dacă rezultatul criptării este identic cu cel recepționat de la client, se realizează autentificarea.

Vulnerabilitatea în acest proces constă în faptul că se poate utiliza criptanaliza folosind perechea de texte în clar şi criptat interceptate pentru a determina cheia secretă RC4. Pe internet se poate găsi cu uşurință un program numit AirSnot cu ajutorul căruia se poate sparge criptarea WEP şi mesajele pot fi citite.

3. Îmbunătățirea securității WEP

Ca urmare a vulnerabilităților din securitatea WEP, a fost lansat un standard complet nou, **802.11i**, care conține o criptare WEP îmbunătățită şi o metodă de asigurare a integrității numită *Protocol de Integritate cu Cheie Temporară* (TKIP). Datorită numărului mare de echipamente mobile fără fir existente la data lansării noului standard care foloseau funcții WEP implementate hardware, a fost aleasă soluția implementării TKIP ca şi un upgrade software la sistemele de bază.

TKIP foloseşte pentru schimbul securizat de chei arhitectura de autentificare 802.1X, care la rândul său se bazează pe *Protocolul de Autentificare Extensibil* (EAP) şi pe protocolul de transport RFC 2284. Pentru rețelele fără fir, protocolul EAP este cunoscut şi ca EAPOL. EAPOL este folosit pentru schimbul de întrebări şi răspunsuri între stațiile client şi un server de autentificare. A treia entitate în 802.1X este *autentificatorul*, un port de control cu acces dual, similar cu un punct de acces. Întrucât 802.1X nu a eliminat vulnerabilitățile generate de vectorul de inițializare IV, TKIP încearcă să corecteze aceasta, ca şi alte vulnerabilități ale securității WEP.

În tabelul 1, sunt prezentate îmbunătățirile aduse de TKIP ca urmare a tratării vulnerabilităților existente în sistemul de securitate WEP.

Tabelul 1

Vulnerabilități WEP	TKIP
Combinația IV şi chei slabe	Funcția de mixare a cheilor per-pachet
Vulnerabilitatea la atacurile de tip răspuns	Disciplina de succesiune a IV
Refolosirea cheilor	Structura ierarhică de chei
Vulnerabilitatea la atacurile de tip imitare	Codul de Integritate a Mesajului (MIC)

3.1. Funcția de mixare a cheilor per-pachet corectează vulnerabilitatea cauzată de combinația dintre IV şi cheile slabe utilizate în WEP prin utilizarea cheilor variabile în timp ca şi chei secrete WEP. Astfel, pentru construirea cheilor secrete şi a vectorului de inițializare per-pachet, se utilizează numărul de ordine a pachetului şi o cheie temporară care, împreună

cu adresa MAC locală, generează cheile intermediare diferite pentru fiecare stație client. Rezultatul întregului proces este un pachet de 16 octeți care corespunde mecanismului WEP implementat hardware în echipamentele existente. (fig.3)

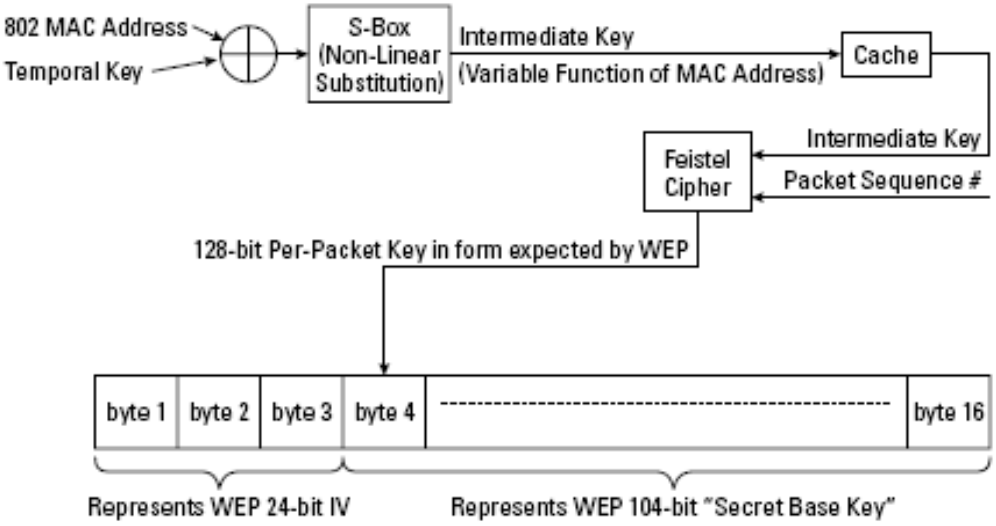

Fig.3

3.2. Disciplina de succesiune a IV reprezintă o măsură împotriva atacurilor de tip răspuns, prin care destinatarul determină dacă un pachet este în afara ordinii normale, caz în care pachetul este ignorat. În acest mod, câmpul WEP pentru IV (24 biți) este utilizat ca si număr de ordine al pachetului, resetat ori de câte ori se utilizează noi chei TKIP şi incrementat de emițător la fiecare pachet transmis.

3.3. Codul de Integritate a Mesajului (MIC) este o reprezentare unică şi neambiguă a mesajului transmis care se schimbă dacă orice bit al mesajului este schimbat (fig.4). Codul este calculat de emițător şi atașat mesajului, iar receptorul calculează MIC şi îl compară cu cel recepționat. Dacă cele două MIC sunt identice, teoretic mesajul nu a fost modificat în timpul transportului.

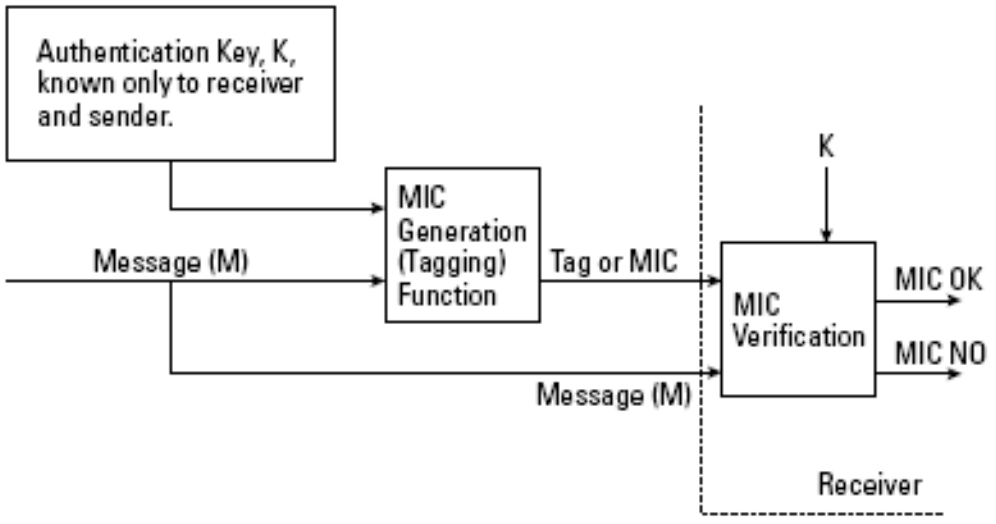

Fig. 4

3.4. Structura ierarhică de chei se compune din chei master, chei de criptare a cheilor şi chei temporare. Cheile temporare 802.1X sunt utilizate în procesele de autentificare şi confidenţialitate TKIP. Un set de chei temporare se compune dintr-o cheie de 64 biţi pentru procesul MIC şi o cheie de criptare de 128 biţi. Pentru fiecare asociere se generează un set diferit de chei temporare. Informaţia folosită pentru generarea cheilor temporare se protejează pentru a nu fi compromisă cu ajutorul cheilor de criptare a cheilor. Cheia master este necesară pentru stabilirea cheilor de criptare a cheilor.(fig.5)

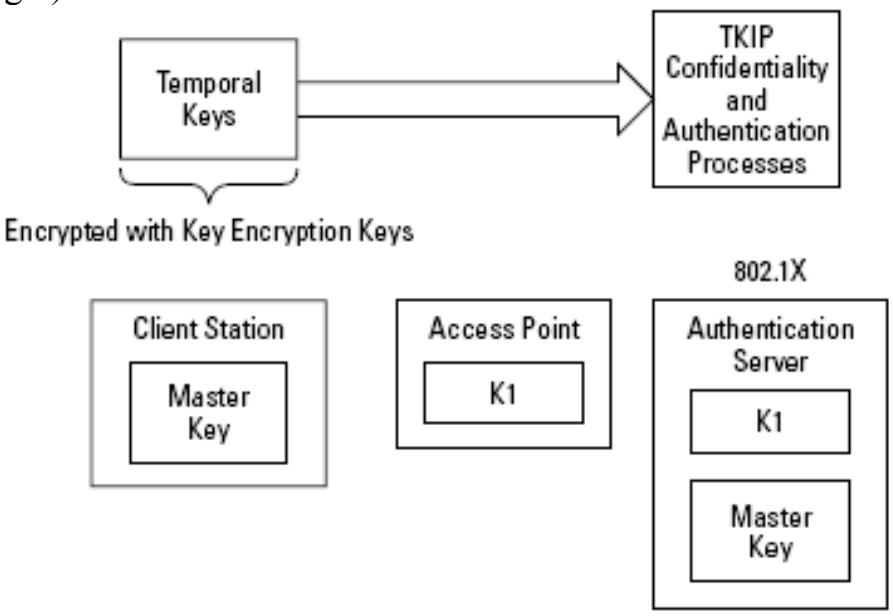

Fig.5

Structura ierarhică de chei se descrie astfel:

- Standardul 802.1X stabileşte că serverul de autentificare şi staţiile client folosesc aceeaşi cheie secretă – cheia master;
- Standardul 802.1X stabileşte că serverul de autentificare şi punctele de acces folosesc aceeaşi cheie secretă determinată de serverul de autentificare pentru fiecare staţie client şi distribuită punctelor de acces de către serverul de autentificare;
- Pentru fiecare sesiune se utilizează o nouă cheie master (o sesiune durează din momentul autentificării până în momentul când cheia expiră, este revocată sau staţia client nu mai comunică);
- Cheia master este folosită pentru a proteja transmiterea cheilor de criptare a cheilor între staţiile client şi punctele de acces;
- Cheile de criptare a cheilor sunt utilizate pentru protejarea informaţiilor utilizate de punctele de acces şi de staţiile client pentru generarea cheilor temporare;
- Perechile de chei temporare sunt folosite pentru protejarea integrităţii şi confidenţialităţii datelor.

4. Standardul 802.11i

Standardul de securitate pentru rețele fără fir 802.11i a fost adoptat în iunie 2004. Comitetul IEEE 802.11 consideră aceste specificații ca fiind o soluție pe termen lung, care încorporează TKIP, 802.1X şi Standardul Avansat de Criptare (AES). AES este un cifru bazat pe blocuri care procesează textul clar în blocuri de 128 biți, cu folosirea următorului set de chei:

- O cheie master simetrică – deținută de serverul de autentificare şi de stațiile client pentru stabilirea accesului;
- O pereche de chei master (PMK) – deținute de punctul de acces şi de stațiile client pentru autorizarea accesului la mediul de comunicație 802.11;
- O pereche de chei tranzitorii (PTK) – compusă din următoarele chei operaționale:
  - Chei de criptare a cheilor – folosite pentru distribuirea cheilor tranzitorii de grup (GTK) utilizate pentru protejarea datelor multicast şi broadcast;
  - Chei de confirmare a cheilor – transmit PMK la stațiile client şi la punctele de acces;
  - Chei temporare(TK) – protejează datele transmise.

Standardul 802.11i implică utilizarea cheilor de 128 biți, combină criptarea şi autentificarea, foloseşte chei temporare pentru ambele procese şi protejează întregul pachet 802.11i.

5. Bluetooth

Bluetooth este un protocol punct-la-punct, de rază scurtă, utilizat pentru conectarea telefoanelor celulare, laptopurilor, pda-urilor, camerelor digitale, imprimantelor, etc. Este definit prin standardul IEEE 802.15, cu următoarele caracteristici:

- Frequency Hopping Spread Spectrum (FHSS) – 1600 Hops pe secundă, cu 79 canale radio;
- Rata de transmisie – 1 Mbps;
- Raza de transmisie – aproximativ 10 m;
- Banda de frecvențe – 2,4 GHz la 2,5 GHz;
- Puterea de emisie – 1 mW pentru minimizarea interferențelor cu alte rețele;
- Extinderea razei de transmisie până la 100 m prin mărirea puterii de emisie la 100 mW;
- Numărul maxim de dispozitive în rețea – 8.

Datorită utilizării FHSS, în aceeaşi zonă pot coexista mai multe rețele Bluetooth fără interferențe mutuale. Dispozitivele Bluetooth funcționează prin stabilirea unei rețele locale personale (PAN), numită *piconet*, bazată pe

adresele asignate dispozitivelor. O rețea piconet Bluetooth funcționează astfel:

- Ca o rețea ad-hoc;
- Toate dispozitivele Bluetooth au importanță egală;
- Diferite rețele piconet utilizează secvențe diferite de hopping pentru prevenirea interferențelor;
- Toate dispozitivele din acelaşi piconet sunt sincronizate cu secvența de hopping a rețelei;
- Un dispozitiv acționează ca master iar celelalte dispozitive acționează ca slave (topologie punct-multipunct);
- Maximum 7 dispozitive slave active pot exista într-un piconet, având atribuită o adresă de membru activ pe 3 biți;
- Până la 256 dispozitive inactive (parcate) care sunt sincronizate cu secvența de hopping pot fi asignate la acelaşi piconet. Acestea pot fi activate rapid pentru că sunt sincronizate.

Securitatea Bluetooth foloseşte protocoale întrebare – răspuns pentru autentificare, un cifru pentru criptarea fluxurilor de date şi chei de sesiune alocate dinamic.

Note bibliografice

[1] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, *Network Security Bible*, Wiley Publishing, 2005, pag. 381 – 416
[2] http://grouper.ieee.org/groups/802/11/index.html, *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs*
[3] Rajeev Shorey, A. Ananda, Mun Choon Chan, Wei Tsang Ooi, *Mobile, Wireless, And Sensor Networks Technology, Applications, And Future Directions*, John Wiley & Sons, 2006, pag. 29 – 44, 283 – 304