MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef departament:

Fiodorov Ion, conf. univ., dr.

_____

„ ____”_____2022

Securizarea avansată a rețelelor WiFi din cadrul rețelelor corporative

Teză de master

Student: **Ciubotaru Vadim, SI-211M**

Conducător: **Moraru Victor, dr., conf.univ.**

Chișinău 2022

ADNOTARE

La proiectul de master: „ Securizarea avansată a rețelelor WiFi din cadrul rețelelor corporative”,

elaborat de Ciubotaru Vadim, Chișinău 2022.

Cuvinte cheie: Rețele WiFi, rețele corporative, securitatea rețelelor.

Scopul lucrării este studierea vulnerabilităților principale ale rețelelor WiFi(IEEE 802.11) a mecanismelor de securitate tradiționale și a metodelor de securizare specifice în cadrul unei rețele corporative .

Obiectivele proiectului sunt: studierea literaturii de specialitate: studierea și analiza mecanismelor actuale de securitate din rețelele WiFi, studierea și testarea practică a atacurilor principale în rețelele WiFi, studierea specificului securizării rețelelor în cadrul rețelelor corporative (autorizare centralizată, monitorizarea traficului, detectarea intruziunilor, etc.), implementarea în practică a atacurilor pentru a demonstra slăbiciunile și limitele metodelor tradiționale de securizare WiFi și propunerea și testarea unei metodologii complexe pentru securizarea rețelelor WiFi corporative.

Tehnologiile utilizate sunt: WPA2-Enterprise

Memoriul explicativ conţine: introducere, 3 capitole, concluzii, bibliografie cu 35 titluri, dintre care 72 pagini text de bază, 63 figuri, 0 tabele.

Capitolul 1: Va informa despre caracteristicele rețelele corporative, tipurile de securizare a rețelelor, avantajele și dezavantajele rețelelor corporative, vulnerabilitățile și atacurile asupra rețelelor, necesitatea de îmbunătățire a nivelului de securizare a rețelelor corporative.

Capitolul 2: Descrie mediul de dezvoltare a proiectului și analiza arhitecturii. Definește tehnicele și metodele aplicate pentru implementarea proiectului.

Capitolul 3: Descrie structura completă a aplicației, configurarea proiectului, descrierea algoritmilor aplicației.

ANNOTATION

For the master's project: " Advanced security of WiFi networks as part of corporate networks ",
elaborated by Ciubotaru Vadim, Chișinău 2022.

Keywords: WiFi networks, corporate networks, network security.

The aim of the paper is to study the main vulnerabilities of WiFi networks (IEEE 802.11), traditional security mechanisms and specific security methods within a corporate network.

The objectives of the project are: study of specialized literature: study and analysis of current security mechanisms in WiFi networks, study and practical testing of main attacks in WiFi networks, study of the specifics of network security within corporate networks (centralized authorization, traffic monitoring, intrusion detection, etc.) .), the practical implementation of attacks to demonstrate the weaknesses and limits of traditional WiFi security methods, and the proposal and testing of a complex methodology for securing corporate WiFi networks.

The technologies used are: WPA2-Enterprise

The explanatory memorandum contains: introduction, 3 chapters, conclusions, bibliography with 35 titles, of which 72 pages of basic text, 63 figures, 0 tables.

Chapter 1: It will inform about the characteristics of corporate networks, types of network security, advantages and disadvantages of corporate networks, vulnerabilities and attacks on networks, the need to improve the level of security of corporate networks.

Chapter 2: Describes the project development environment and the analysis of the architecture. Defines the techniques and methods applied for project implementation.

Chapter 3: Describes the complete structure of the application, the configuration of the project, the description of the application algorithms.

CUPRINS

Introducere

În ultimele două secole tehnologiile au avansat foarte mult, încât sunt prezente peste tot în viața noastră. Aceste tehnologii sunt utilizate practic în toate domeniile pentru a avea o performanță mai mare în realizarea unei sarcini și pentru a ușura viața omului. Unul dintre domeniile importante, în care sunt utilizate aceste tehnologii este cel rețelistic. Rețeaua este despre stabilirea și cultivarea de relații reciproc avantajoase pe termen lung cu oamenii pe care îi întâlnești, indiferent dacă aștepți să-ți comanzi cafeaua de dimineață, să participi la o ligă sportivă intramurală sau să participi la o conferință de lucru.

În ultimul timp în Republica Moldova, rețelistica a luat țara cu asalt și treptat se dezvoltă la nivel național din toate punctele de vedere. De aceea rețelistica la etapa actuală în țara noastră prezintă un avantaj major, care constituie un suport, care vă ajută să vă dezvoltați și să vă îmbunătățiți setul de abilități, să fiți la curent cu ultimele tendințe din industria dvs., să păstrați un impuls pe piața muncii, să întâlniți mentori potențiali, parteneri și clienți și să obțineți acces la resursele necesare care vă vor încuraja dezvoltarea carierei.

Teza de masterat este dedicată pe studierea securizării rețelelor de WiFi instituționale și sporirea gradului de securitate în cazul unui atac. Rețelele wireless sunt relativ mai puțin sigure decât cele cablate datorită accesului mai facil la rețea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. Există implicit în implementarea retelelor wireless diferite bariere care formează așa numita securitate de baza a rețelelor wireless, care împiedică accesul neintenționat al persoanelor străine de rețea aflate în aria de acoperire a unui punct de acces. Pentru persoane rău intenționate, cu bună pregătire în domeniu, de tipul hackerilor, securitatea acestor rețele ca de altfel și a altora este discutabilă.

Din perspectiva dezvoltatorului, toate acestea sunt garantate pentru a fi consecvente, indiferent de locul în care aplicația este implementată în cele din urmă. Toate acestea se traduc prin productivitate: dezvoltatorii și echipele IT Ops petrec mai puțin timp depanând și diagnosticând diferențele în medii și mai mult timp livrând noi funcționalități pentru utilizatori. Și înseamnă mai puține bug-uri, deoarece dezvoltatorii pot acum face presupuneri în medii de dezvoltare și testare, pot fi siguri că vor fi adevărate în producție.

O rețea fără fir sau WiFi utilizează un semnal de frecvență radio în loc de fire pentru a vă conecta dispozitivele - cum ar fi computere, imprimante și smartphone-uri - la internet și între ele. Semnalul WiFi poate fi preluat de orice dispozitiv compatibil wireless, cum ar fi un laptop sau o tabletă, la o anumită distanță, în toate direcțiile. Deoarece dispozitivele WiFi

folosesc un semnal de difuzare în loc de fire pentru a se conecta la Internet și a învăța pe alții, este posibil ca utilizatorii neautorizați să vă acceseze rețeaua. Acest lucru ar putea reduce viteza conexiunii sau vă poate face vulnerabil la lucruri precum furtul de identitate. Cu toate acestea, există mai multe moduri de a vă asigura că rețeaua dvs. wireless de acasă este sigură.

În ceea ce privește testarea rețelei, rețeaua dvs. Wi-Fi este conexiunea la internet wireless a casei dumneavoastră, sau în instituția unde activați la moemntul dat. De obicei implică un router wireless care trimite un semnal prin aer. Puteți folosi acel semnal pentru a vă conecta la internet. Dar, cu excepția cazului în care rețeaua dvs. este protejată prin parolă, orice dispozitiv din raza de acțiune poate trage semnalul din aer și vă poate folosi conexiunea la internet.

Ca inginer de rețea, o aplicație configurată necorespunzător poate costa mult timp și bani pe linie. Cel mai bun mod de a încerca și de a preveni aceste accidente nefericite este prin efectuarea de teste amănunțite și eficiente pe o bază de rutină. În ceea ce privește testarea rețelei, termenii de emulare și simulare sunt adesea folosiți interschimbabil. În majoritatea cazurilor, oricare dintre termeni va obține, în general, ideea, dar există o mare diferență între un emulator de rețea și un simulator de rețea, atât practic, cât și semantic.

Scopul lucrării este studierea vulnerabilităților principale ale rețelelor WiFi(IEEE 802.11) a mecanismelor de securitate tradiționale și a metodelor de securizare specifice în cadrul unei rețele instituționale.

Obiectivele proiectului sunt: studierea literaturii de specialitate: studierea și analiza mecanismelor actuale de securitate din rețelele WiFi, studierea și testarea practică a atacurilor principale în rețelele WiFi, studierea specificului securizării rețelelor în cadrul rețelelor instituționale (autorizare centralizată, monitorizarea traficului, detectarea intruziunilor, etc.), implementarea în practică a atacurilor pentru a demonstra slăbiciunile și limitele metodelor tradiționale de securizare WiFi și propunerea și testarea unei metodologii complexe pentru securizarea rețelelor WiFi instituționale.

1. ANALIZA SITUAȚIEI ÎN DOMENIUL PROIECTĂRII

1.1 Rețeaua WiFi

1.1.1 Prezentare generală a rețelei WiFi

Ce este rețeaua WiFi

Wi-Fi este o tehnologie de rețea fără fir care permite dispozitivelor precum computere (laptop-uri și desktop-uri), dispozitive mobile (telefoane inteligente și dispozitive portabile) și alte echipamente (imprimante și camere video) să interfațeze cu Internetul. Permite acestor dispozitive - și multe altele - să facă schimb de informații între ele, creând o rețea. Conexiunea la internet are loc printr-un router wireless. Când accesați Wi-Fi, vă conectați la un router fără fir care permite dispozitivelor dvs. compatibile cu Wi-Fi să interacționeze cu Internetul. [1]

Etimologie și terminologie

Denumirea Wi-Fi, folosită comercial cel puțin încă din august 1999, a fost inventată de firma de consultanță de brand Interbrand. Wi-Fi Alliance a angajat Interbrand pentru a crea un nume care să fie „puțin mai captivant decât „IEEE 802.11b Direct Sequence". Potrivit lui Phil Belanger, membru fondator al Wi-Fi Alliance, termenul Wi-Fi a fost ales dintr-o listă de zece nume propuse de Interbrand.Alianța Wi-Fi a folosit sloganul publicitar „Standardul pentru fidelitatea fără fir" pentru o scurtă perioadă de timp după ce a fost creat numele mărcii, iar Alianța Wi-Fi a fost numită și „Alianța pentru fidelitate fără fir". Inc" în unele publicații. Numele este adesea scris ca WiFi, Wifi sau wifi, dar acestea nu sunt aprobate de Wi-Fi Alliance. IEEE este o organizație separată, dar înrudită, iar site-ul lor web a declarat „WiFi este un nume scurt pentru Wireless Fidelity". Interbrand a creat și sigla Wi-Fi. Sigla Wi-Fi yin-yang indică certificarea unui produs pentru interoperabilitate. Alte tehnologii destinate punctelor fixe, inclusiv Motorola Canopy, sunt de obicei numite fără fir fix. Tehnologiile wireless alternative includ Zigbee, Z-Wave, Bluetooth și standardele pentru telefoane mobile, cum ar fi 2G, 3G, 4G, 5G și LTE. [4]

1.1.2 Tipuri de rețele WiFi

Există patru tipuri de rețele wireless -- rețele locale fără fir, rețele wireless de zonă metropolitană, rețele wireless de zonă personală și rețele wireless de zonă largă -- fiecare cu propria sa funcție. Mai jos discutăm despre diferitele tipuri de rețele fără fir și despre diferitele echipamente și conexiuni de care au nevoie.

Wireless LAN

Tehnologia LAN fără fir (WLAN) oferă acces la internet într-o clădire sau într-o zonă exterioară limitată. Folosită pentru prima dată în birouri și case, tehnologia WLAN este acum

folosită și în magazine și restaurante. Utilizarea rețelelor de acasă a crescut foarte mult, deoarece pandemia de COVID-19 a forțat lucrătorii de birou, studenții, profesorii și alții să lucreze și să studieze de acasă. Majoritatea modelelor de rețele de acasă sunt simple. Un modem se conectează la cablu sau fibră de la un furnizor de servicii local. Un router wireless este conectat la modem și primește semnalul de la modem, pe care apoi îl transmite folosind un protocol fără fir, cum ar fi standardele 802.11. Rețelele de birouri sunt mai complicate. Punctele de acces (AP) sunt montate pe tavan, fiecare difuzând un semnal wireless în zona înconjurătoare. Sunt necesare mai multe AP-uri în birourile mari, fiecare conectându-se la rețeaua centrală a biroului printr-o conexiune prin cablu la un comutator.

Wireless MAN

Rețelele wireless din zona metropolitană au fost instalate în orașe din întreaga lume pentru a oferi acces persoanelor din afara unei rețele de birou sau de acasă. Aceste rețele acoperă o zonă mai largă decât rețelele de birou sau de acasă, dar principiile sunt aceleași. AP-urile sunt amplasate pe părțile laterale ale clădirilor sau pe stâlpi de telefon în întreaga zonă de acoperire. AP-urile sunt conectate la internet printr-o rețea cu fir și transmit un semnal fără fir în întreaga zonă. Utilizatorii se conectează la destinația dorită conectându-se la cel mai apropiat AP, care redirecționează conexiunea prin conexiunea sa la internet.

Wireless PAN

Rețelele personale fără fir acoperă o zonă foarte limitată -- de obicei maximum 100 de metri pentru majoritatea aplicațiilor -- folosind protocoale precum Bluetooth și Zigbee. Bluetooth permite apeluri telefonice fără mâini, conectează un telefon la căști sau transmite semnale între dispozitive inteligente. Zigbee conectează stațiile de-a lungul unei rețele IoT. Tehnologia cu infraroșu este limitată la linia de vedere, cum ar fi conectarea telecomenzilor TV la televizoare. Dezvoltatorii wireless au îmbunătățit constant tehnologia prin descoperirea de noi modalități de a transmite semnale către utilizatori. Aceste progrese permit rate de date mai mari și o rază de acțiune mai mare pentru fiecare dintre aceste tehnologii wireless.

Wireless WAN

Rețelele WAN fără fir utilizează tehnologia celulară pentru a oferi acces în afara domeniului unei rețele LAN fără fir sau a unei rețele metropolitane. Aceste rețele permit utilizatorilor să efectueze apeluri telefonice către alte persoane care se conectează fie printr-un WAN fără fir, fie printr-un sistem de telefonie cu fir. De asemenea, utilizatorii se pot conecta la internet pentru a accesa site-uri web sau aplicații bazate pe server.Turnurile celulare sunt situate aproape peste tot în SUA și în majoritatea altor țări. O conexiune de utilizator este direcționată către cel mai apropiat turn de telefonie mobilă care, la rândul său, este conectat fie la internet prin cablu, fie la un alt turn conectat la internet prin cablu.

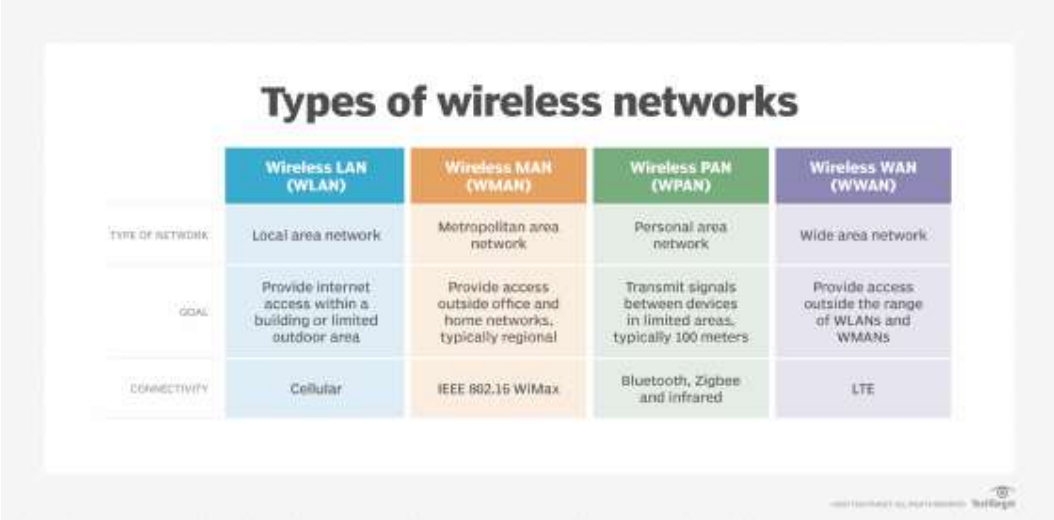

Figura 1.1 Tipuri de rețea fără fir[12]

1.1.3 Funcționalitatea rețelei WiFi și tipurile de acces

Din punct de vedere tehnic, standardul IEEE 802.11 definește protocoalele care permit comunicațiile cu dispozitivele wireless actuale compatibile cu Wi-Fi, inclusiv routere wireless și puncte de acces wireless. Punctele de acces wireless acceptă diferite standarde IEEE. Fiecare standard este un amendament care a fost ratificat de-a lungul timpului. Standardele funcționează pe frecvențe diferite, oferă lățime de bandă diferită și acceptă un număr diferit de canale.

Ce este un punct de acces wireless?

Un punct de acces fără fir (AP) permite dispozitivelor fără fir să se conecteze la rețeaua fără fir. Având o rețea fără fir Cisco, este ușoară aducerea de noi dispozitive online și oferă asistență flexibilă lucrătorilor mobili. Ceea ce face un punct de acces wireless pentru rețeaua dvs. este similar cu ceea ce face un amplificator pentru stereo de acasă. Un punct de acces preia lățimea de bandă care vine de la un router și o întinde astfel încât multe dispozitive să poată intra în rețea de la distanțe mai mari. Dar un punct de acces wireless face mai mult decât pur și simplu extinde Wi-Fi. De asemenea, poate oferi date utile despre dispozitivele din rețea, poate oferi securitate proactivă și poate servi multor alte scopuri practice.

Ce este un router wireless?

Routerele wireless se găsesc de obicei în case. Sunt dispozitivele hardware pe care furnizorii de servicii de internet le folosesc pentru a vă conecta la rețeaua lor de internet prin cablu sau xDSL.Un router fără fir este uneori denumit dispozitiv de rețea locală wireless (WLAN). O rețea fără fir se mai numește și rețea Wi-Fi.Un router wireless combină funcțiile de rețea ale unui punct de acces fără fir și ale unui router. Citiți mai multe despre routere wireless.

Ce este un router Wi-Fi pentru desktop?

Cea mai obișnuită modalitate prin care utilizatorii se conectează la Internet fără fir este cu un router wireless (Wi-Fi) pentru desktop. Aceste routere arată ca niște cutii mici cu mai multe antene scurte pentru a ajuta la difuzarea semnalului în întreaga casă sau la locul de muncă. Cu cât un utilizator este mai departe de routerul Wi-Fi de bază, cu atât semnalul este mai slab. Așadar, mai multe routere wireless, numite range extenders, sunt de obicei plasate în spațiul de lucru. Extensoarele de rază Wi-Fi, plasate într-o matrice, măresc sau extind acoperirea la internet.

Ce este un hotspot mobil?

Un hotspot mobil este o caracteristică comună pe smartphone-urile cu conexiuni atât legate, cât și fără legătură. Când porniți hotspot-ul mobil al telefonului dvs., vă partajați conexiunea de rețea fără fir cu alte dispozitive care pot accesa apoi Internetul.

Ce este un hotspot Wi-Fi portabil?

Un hotspot Wi-Fi portabil este un hotspot mobil obținut printr-un operator de telefonie mobilă. Este un dispozitiv mic care folosește turnuri celulare care difuzează semnale de bandă largă 3G sau 4G de mare viteză. Mai multe dispozitive, cum ar fi iPad-urile și laptopurile, se pot conecta apoi fără fir la dispozitiv, care, la rândul său, se conectează fără probleme la internet oriunde călătorești. Similar unui telefon mobil, costul lunar al hotspot-ului portabil se bazează pe planul de utilizare a datelor pe care îl selectați. Un hotspot Wi-Fi portabil este o modalitate mai fiabilă de a accesa Internetul decât căutarea de hotspot-uri Wi-Fi publice statice.

1.1.4 Standarde de rețea fără fir

Institutul de Ingineri Electrici și Electronici (IEEE) a creat standardul pentru tehnologia Wi-Fi pe care îl urmează toate routerele wireless, 802.11. Standardul 802.11 se aplică mai multor specificații ale rețelelor WLAN și definește o interfață over-the-air între un client wireless și o stație de bază sau între doi clienți wireless.

Cele cinci tehnologii Wi-Fi sunt A, B, G, N și AC. B și G folosesc frecvența de 2,4 GHz; A și AC folosesc frecvența de 5 GHz; iar N folosește atât frecvențe de 2,4, cât și 5 GHz. Alegerea ta pentru casa sau afacerea ta se va reduce la trei: Wireless G, N sau AC. Routerele care acceptă numai Wireless B nu mai sunt fabricate.

Routerele wireless AC sunt cea mai bună opțiune pentru utilizarea în afaceri mici, deoarece au o capacitate bună de difuzare și permit ca mai multe dispozitive să se bucure de performanțe optime în același timp. În funcție de routerul pe care îl alegeți, vă puteți bucura de funcții de securitate suplimentare și de capabilități de găzduire a serverului.

Routerele wireless N sunt o alegere bună pentru o rețea fără fir de birou de acasă. Aceștia acceptă mai multe computere și alte dispozitive electronice simultan, astfel încât routerul va continua să funcționeze chiar și atunci când rulează computere, sisteme de divertisment și alte elemente periferice simultan.

Routerele wireless G nu sunt o alegere bună pentru birourile mici dacă trebuie să conectați o mulțime de dispozitive între ele sau trebuie să utilizați programe complexe sau aplicații cloud pe internet.

Înainte de a cumpăra un router fără fir, veți dori să vă asigurați că interfețele wireless de pe dispozitivele dvs. acceptă tehnologia aleasă. Nu toate dispozitivele acceptă Wireless AC, de exemplu.

Identificarea rețelei wireless potrivite și a componentelor sale necesare poate fi o călătorie confuză și întortocheată. Pentru birourile de acasă și întreprinderile mici, WLAN este calea de urmat datorită capacităților sale de rază mai bună, iar routerele wireless AC oferă posibilitatea de a conecta mai multe dispozitive la rețea fără a avea loc încetinirea.[12]

1.2 Securizarea rețelei WiFi

1.2.1 Prezentarea generală

Securitatea Wi-Fi este protecția dispozitivelor și a rețelelor conectate într-un mediu wireless. Fără securitate Wi-Fi, un dispozitiv de rețea, cum ar fi un punct de acces fără fir sau un router, poate fi accesat de oricine care utilizează un computer sau un dispozitiv mobil în raza de acțiune a semnalului wireless al routerului. Atunci când dispozitivele wireless dintr-o rețea sunt „deschise” sau nesecurizate, acestea sunt accesibile oricărui dispozitiv compatibil Wi-Fi, cum ar fi un computer sau un smartphone, care se află în raza de acțiune a semnalelor lor wireless. Utilizarea rețelelor deschise sau nesecurizate poate fi riscantă pentru utilizatori și organizații. Adversarii care folosesc dispozitive conectate la internet pot colecta informațiile personale ale utilizatorilor și pot fura identitățile, pot compromite date financiare și alte date sensibile de afaceri, pot „asculta cu urechea” comunicațiilor și multe altele. Securitatea rețelei fără fir protejează în primul rând o rețea fără fir de încercările de acces neautorizate și rău intenționate. De obicei, securitatea rețelei fără fir este furnizată prin dispozitive fără fir (de obicei, un router/comutator fără fir) care criptează și securizează toate comunicațiile fără fir în mod implicit. Chiar dacă securitatea rețelei wireless este compromisă, hackerul nu poate vedea conținutul traficului/pachetului în tranzit. În plus, sistemele de detectare și prevenire a

intruziunilor fără fir permit, de asemenea, protecția unei rețele fără fir, alertând administratorul rețelei fără fir în cazul unei încălcări a securității.[5]

1.2.2 Tipurile de protocoale de securitate wireless

Există patru protocoale principale de securitate fără fir. Aceste protocoale au fost dezvoltate de Wi-Fi Alliance, o organizație care promovează tehnologiile wireless și interoperabilitatea. Grupul a introdus trei dintre protocoalele, descrise mai jos, la sfârșitul anilor 1990. De atunci, protocoalele au fost îmbunătățite cu o criptare mai puternică. Cel de-al patrulea protocol a fost lansat în 2018.

WEP

Primul protocol de securitate wireless a fost WEP (Wired Equivalent Privacy). A fost metoda standard de a asigura securitatea rețelei fără fir de la sfârșitul anilor 1990 până în 2004. WEP a fost greu de configurat și a folosit doar criptare de bază (64-/128-bit). WEP nu mai este considerat sigur și ar trebui înlocuit cu un protocol mai nou, cum ar fi WPA2, descris mai jos.

WPA

WPA (Wi-Fi Protected Access) a fost dezvoltat în 2003. Oferă o criptare mai puternică (128-/256 de biți) decât WEP prin utilizarea unui protocol de securitate cunoscut sub numele de Temporal Key Integrity Protocol (TKIP). Alături de WPA2, WPA este cel mai frecvent protocol utilizat astăzi. Dar, spre deosebire de WPA2, este compatibil cu software-ul mai vechi.

WPA2

WPA2, o versiune ulterioară a WPA, a fost dezvoltată în 2004. Este mai ușor de configurat și oferă o securitate și mai mare a rețelei decât WPA prin utilizarea unui protocol de securitate cunoscut sub numele de Advanced Encryption Standard (AES). Versiunile protocolului WPA2 sunt disponibile pentru utilizatori individuali și întreprinderi.