UNIVERISTETI I PRISHTINËS

FAKULTETI I INXHINIERISË ELEKTRIKE DHE KOMPJUTRIKE

Departamenti i Telekomunkiacionit-Studimet Master

WLAN Security

Arian Halimi & Premton Fetahu

Abstrakti

Ky punim përshkruan me fjalë të shkurtra WLAN Security. WLAN dhe aplikacionet Wireles janë duke u rritur dita ditës në masë të madhe dhe janë duke u bërë mjaft popullore. Ato janë mjaftë të përdorshme dhe shumë të fuqishme, por sa i përket sigurisë ato janë akoma larg nivelit të optimumit. Problemi 'WLAN Security' vazhdon që të jetë 'therra kryesore' e implementimit të tij. Në vazhdim të këtij punimi do të jepen disa informacione lidhur me sigurinë e rrjetave WLAN. Me theks të veçantë është shpjeguar për protokollin 802.11x si nivel i sigurisë dhe WPA-në.

Hyrje

Rrjetat WLAN apo standardi 802.11x e kanë zanafillën kah fundi i viteve 70-ta dhe fillimi i viteve 80-ta, kur edhe filloi zhvillimi i modemeve wireless [Wikipedia]. Këta modem fillimisht kishin shpejtësi shume të ulet përafërsisht rreth (9.6 kbps) dhe distance të vogël transmetimi. Performancat e kësaj teknologjie filluan të përmirësohen me përdorimin e teknologjive të ndryshme moduluese siç ishte spread spectrum (gjenerata e dyte e modemeve wirless). Kurse gjenerata e tretë e modemeve arrin shpejtësin disa Mbps.
Me WLAN nënkuptohet komunikimin në mes të shfrytëzuesve pa tela përmes mediumit transmetues, ajrit (valët elektromagnetike). Aplikimi i WLAN në mjedise të ndryshme si shtëpi, zyra, kamupse, universitete etj i ka përparësitë, por gjithashtu edhe mangësitë e veta. Përparësitë

e përdorimit të WLAN janë: shfrytëzuesve i mundësohet qasje në resurse të ndryshme (Internet, intranet) pa tela, mundësin e lëvizshmërisë nëpër zonën ku mbulohet me WLAN dhe nuk nevojite që të shtrihen kabllo për kyçje me çka ulet edhe kostoja e shpenzimeve etj.
Njeri nga disavantazhët e WLAN-it është siguria e tij. Përderisa te rrjetat me kabllo informacionet nga mediumi transmetues nuk mund te komprimiohen pa pasur qasje fizike, në WLAN kjo mund të ndodh për shkak se informacionet barten përmes valëve.
Për rreziqet si dhe masat preventive që duhet të merren për sigurinë e WLAN do të diskutohet në vazhdim.
Mungesa e lidhjes fizike në mes nyjeve ka mundësuar që lidhja pa tela të jetë e pa sigurtë. Për të pasur një nivel të sigurisë të përafërt me rrejta ma kabllo standarti IEEE 802.11 ka definuar protokollin WEP (Wired Equivalent Privacy) për të cilin gjithashtu do të bëhet fjalë në vazhdim.
Por fillimisht do të përshkruhet me pak fjalë për Security WLAN me shërbime të certifikuara.

Security WLAN me shërbime të çertifikuara

Shumë organizata kanë provuar që të implementojnë WLAN, por në fakt nuk kanë qenë të suksesshme në implementimin e tij. Pavarësisht nga produktiviteti dhe shumë beneficione që WLAN ofron, siguria e pamjaftueshme ka ndaluar që një numër i madh i organizatave ta ndalojnë implementimin e rrjetave WLAN. Organizata të ndryshme kanë zbatuar protokollin WLAN 802.11 duke përdorur gjithashtu siguri me karakteristika të kufizuara ose nuk kanë përdorur siguri [1] .
Por organizata dhe kompani të mëdha botërore siç është p.sh Microsoft kanë dhënë platforma dhe zgjidhje për implementimin e WLAN security duke e ndarë këtë platformë në tri blloqe krysore; planifikimi, ndërtimi dhe operimi, Figura 1. Ky bllok i planifikimit përshkruan hap pas hapi implementimin e WLAN security dhe të gjitha nën blloqet janë të certifikuara p.sh PKI (Public Key Infrastructure) është i bazuar në platformën Microsoft Windows Server™ 2003, infrastruktura e RADIUS është e bazuar në Microsoft Internet Authentication Service dhe informacionet se si janë të konfiguruar wireless access point. Për më shumë lexuesi mund ti referohet [1]

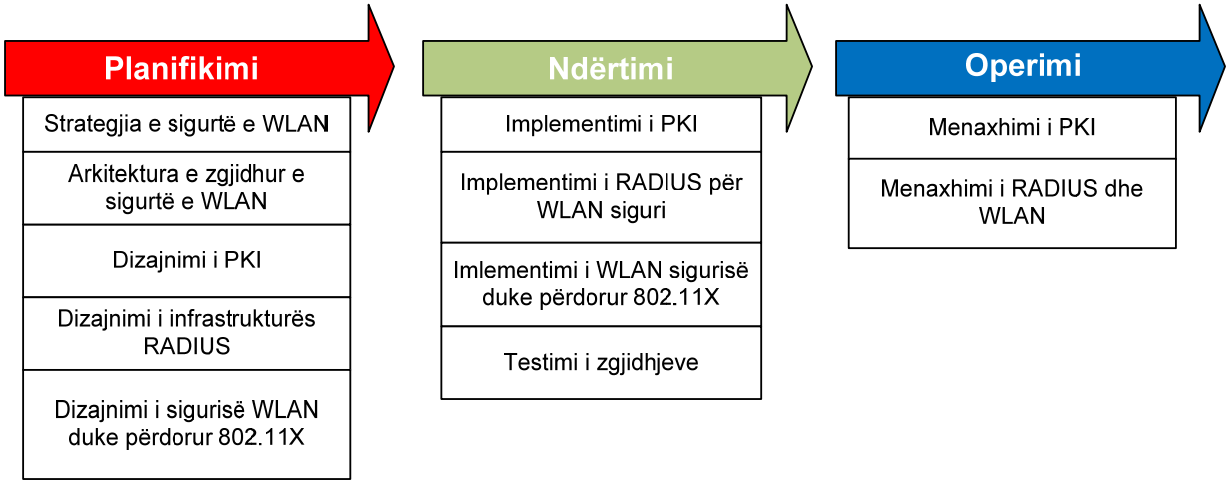

Figura 1 Pamja e sigurisë së rrjetit WLAN me çertifakatë (platforma e Microsoftit)

Transferimi i informacioneve të modifikuara do të thotë që një pjesë e mesazheve është ndryshuar ose vonuar, dhe nuk i duron dot që ti lejoj funksionet e pa dëshiruara dhe të pa autorizuara.
Preventivat totale ose parciale të shërbimeve e bëjnë përdorimin e rrjetit të vështirë. Këto sulme tentojnë që ta ndërprejnë lidhjen e komunikimit ose ta mbingarkojnë rrjetin me shumë mesazhe për ta zvogëluar throughput-in. Në vazhdim janë paraqitur disa nga masat preventive që e mbrojnë rrjetin Wirelesst.

Firewall- e mbronë rrjetin nga përdoruesit e jashtëm, të cilët tentojnë të qasen nga rrjeti me tela. Në çoftë se firewall-i është perfekt atëherë metodat tjera të implementuara mund të gjurmojnë dhe detektojnë passworda-t, pra të userave të jashtëm të trafikut WLAN. Por megjithatë nuk është kaq lehtë sa duket në shikim të parë. Dëmtimi më i madh i një kompanie të rrjetës vjen nga vetë kompania. Pa masat e duhura të sigurisë ndonjëri prej shfrytëzuesve të regjistruar të kompanisë, dhe i cili nuk ka më punë me të njëjtën kompani mund tu qaset të dhënave dhe rrjetit. Ish i punësuari ka ditur se si ti lexoj dhe ti shpërndaj të dhënat e kompanisë [2].

Password-i i rrjetit- kontrolli i rrjetit me password duhet që të implementohet në rastin e rrjetit pa tela. Passwordat duhet të jenë nën një kontroll të fortë dhe të ndryshuar herë pas here. Meqenëse rrjeti WLAN mund ti përshtat përdoruesit mobil, të cilët tentojnë ti lëvizin lap-topët e tyre prej një vendi në një vend tjetër, policia strikte e passwordave e jep edhe një shtresë më tepër për siguri [2].

MAC adresimi- përdoret për autentifikimin e MAC adresës ose paswordat e përdorur. Për ti përdorur këto adresime në rrjetën me shumë vizitor do të duhej të kërkohej shumë fuqi në helpdesk për ti mbajtur të gjitha këto të dhëna [2].

Izolimi- shfrytëzuesit e rrjetit WLAN duhet të dijnë radio domenin, kanalet, nën kanalet, security ID-në dhe paswordin. Në një rrjet Wireless LAN access point-i funksionon si bridge dhe përdorimi i rrjetit në formën e izoluar është i paaftë që ti detektojë paketat e rrjetit back bone [2].

1. WEP (Wired Equivalent Privatcy)

WEP-bënë enkriptimin ndërmjet access point-it wireless dhe klientit wireless. WEP siguron dy çështje kryesore në sigurinë e rrjetave wireless; *autentifikimin* dhe *konfidencialitetin*. Për ti mbrojtur të dhënat WEP-i përdor RC4 chiperin i cili përdor një varg bitash, të quajtur key streams dhe i kombinon këtë me mesazhin për të krijuar chiper tekstin. Çelësi RC4 i cili zakonisht është 64 bitësh përbëhet prej dy pjesëve: 40 bit çelës sekret dhe 24 bita vektor të inicializimit (Inicialization Vector). Ky vektor i inicializimit është një numër i që ndryshon në vazhdimësi dhe përdoret për ti parandaluar sekuencën e tekstit që është e njëjtë me sekuencën paraprake prej krijimit te chipertekstit të njëjtë kur të enkriptohet. Për ta pranuar marrësi sinjalin duhet ta procesoj chipertekstin me një keystream te njëjtë si në dhënës[12]. Hapi i parë që bëhet është gjenerimi i WEP çelësit. Pasi të jetë gjeneruar kjo vlerë ajo vendoset në AP. Në mënyrë që të sigurohet se secili shfrytëzues mund të pranoj dhe deenkriptoj sinjalin, ky çelës duhet vendosur secilit shfrytëzues.. Kur të dhënat janë të gatshme për transmetim çelësi WEP dhe vektori i inicializimit kombinohen, pastaj duke përdorur chiperin RC4, çelësi dhe vektori i

inicializimit përdorin shprehjen logjike XOSE me të dhënat IVC për të krijuar frame-at e enkriptuar Figura 2 [7].

Standardi 802.11 specifikon çelësat 40 bitësh, sidoqoftë shumica e prodhuesve kanë implementuar çelësa 104 bitësh për siguri më të lartë [3,4].

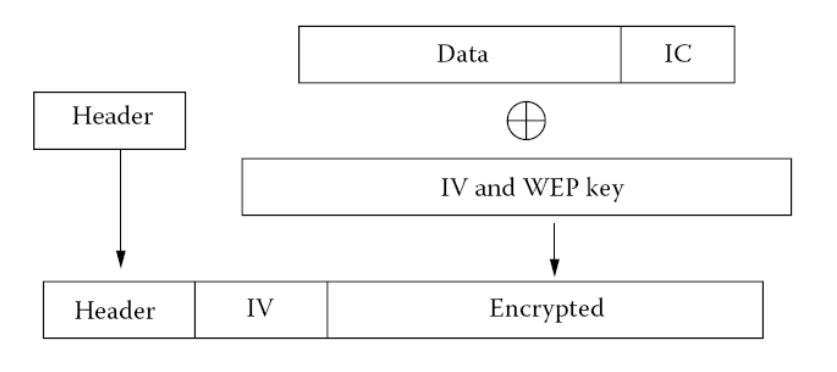

Figura 2 Enkriptimi bazik i WEP-it

WEP ka treguar se ka disa dobësi, të cilat iu lejojnë sulmuesve (hacker) që ti tejkalojnë nivelet e caktuara të kontrollit të sigurisë 802.11. Ekzistojnë disa software, të cilët deshifrojnë çelësat WEP, siç janë Airsnort[1] dhe Webcrack[2], WEP dhe mund të thyhet për 30 minuta ose në qofte se është i bazuar në fjalë të fjalorit, mund të thehet më pak se sa një minutë, informacioni i bazuar në një publikimi shkencor në lidhje me algoritmin RC4 [8]**.**

2. Autentifikimi

Siguria e rrjetave WLAN është element mjaft i rëndësishëm për ti bërë të besueshme dhe të përdorshme këto rrjeta, prandaj si theks i veçantë i kësaj është edhe autentifikimi. Ekzistojnë dy metoda për autentifikimin në baze të standartit IEEE 802.11**:**

- *Shared Key Authentication* dhe
- *Open System Authentication*

Open System Authentication mundëson autentifkimin e të gjithë shfrytëzuesve, të cilët bëjnë kërkesë për qasje në rrjetë [2], rrjeti i autentifikon ata dhe i jep qasje, Figura 3.
Shared Key Authentification është e bazuar në ndarje të çelësave. Shfrytëzuesi i rrjetit wireless pyet për autentifikim dhe ai ia dërgon kërkesën për autentifikim access pointit. AP e dërgon atë prapa si tekst të rëndomtë. Ky tekst enkriptohet nga ana e shfrytëzuesit dhe i dërgohet AP. Nëse teksti i enkriptuar është i pranueshëm prej access point-it atëherë shfrytëzuesi i qaset rrjetit, Figura 4.

[1] http://www.airsnorth.shmoo.com
[2] http://www.wepcrack.sourceforge.net

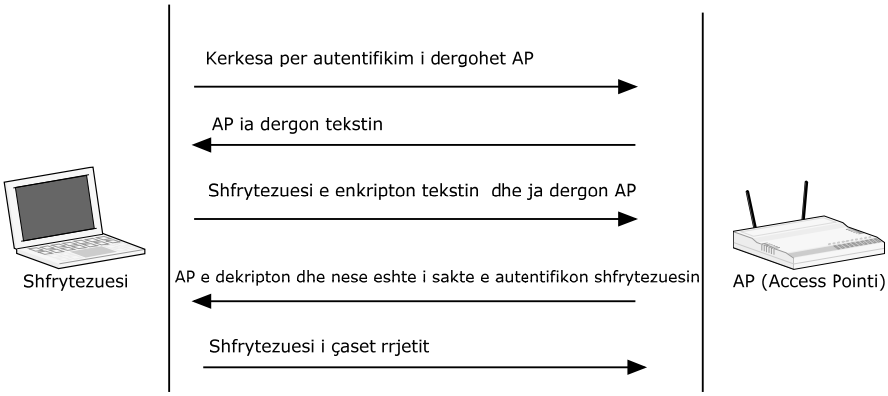

Figura 3 Shared key authentication

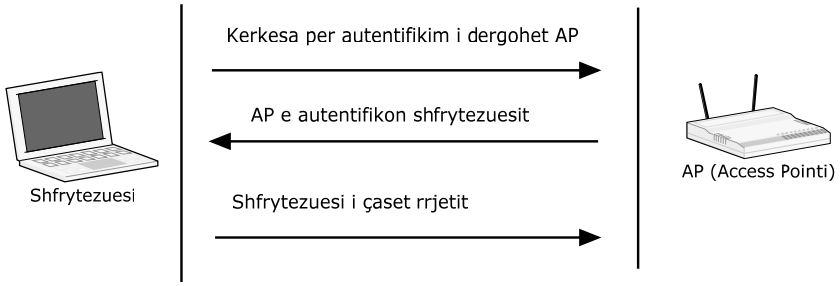

Figura 4. Open system authentication

3. SSID- Service Set Identification

SSID është kod i cili i bashkëngjitet të gjitha paketave në rrjetin wireless, për ta identifikuar secilën pakete si pjesë të atij rrjeti. NIC kartela e Wireless shfrytëzuesit duhet të konfigurohet me SSID të njëjtë sikurse access pointi në mënyrë që të ketë qasje në rrjetë. [6].
Ekzistojnë dy lloje të SSID:

- tek rrejtet Ad-Hoc ku nuk kemi access pointa shfrytëzuesit përdorin IBSSID (Indepedent basic serivece set ID) dhe
- rrjetet që kane access pointa ku përdoret ESSID (Extended SSID). SSID ndryshe njihet edhe si emri i rrjetit (Network Name)

Administratoret e rrjetit zakonisht përdorin SSID publike, që vendosen nëpër access pointa dhe e shpërndanë në të gjitha pajisjet wirless [http://en.wikipedia.org/wiki/SSID].

4. Standardi 802.1x/EAP (Extensible Authentication Protocol)

Me përdorimin standardit IEEE 802.1X ofrohet një strukture efektive për autentifikimin dhe kontrollin e trafikut të shfrytëzuesit në rrjetat e mbrojtura, si dhe ndryshimin e çelësave në mënyrë dinamike. 802.1x definon kontrollin e çasjes të bazuar në portet e rrjetës që përdorin protokollin EAP (Extensible Authentication Protocol) për rrjeta me kabllo dhe Wireless dhe

përkrah metoda të ndryshme të autentifikimit siç janë paswordat, çertifikatat, publik key authentication [10].

802.1x përbehet prej tri elementeve:

- Shfrytezuesit i cili kërkon që të autenifikohet dhe njihet si kërkues (supplicant)
- Serverin i cili e bënë autentifikimin, zakonisht është RADIUS serverit dhe njihet si server i autentifikimit
- Dhe pajisja në mes shfrytëzuesit dhe serverit që është AP dhe njihet si autentifikator.

Komunikimi realizohet ne kete menyre:

Shfrytëzuesi i paautentifikuar tenton t'i qaset një autentifikatori (AP). AP i përgjigjet duke i mundësuar një Port për ti kaluar vetëm paketat e EAP prej klientit tek serveri i autentifikimit i cili gjendet në anën tjetër të rrjetit. AP e bllokon të gjithë trafikun tjetër si p.sh HTTP, POP3, derisa AP ta verifikon identitetin e klientit duke përdorur serverin e autentifikimit (RADIUS serveri). Pasi që të bëhet autentfikimi AP i hap portin e klientit për trafik tjetër [11].

.

Protokolli 802.1x nuk e definon protokollin aktual të autentifikimit por e specifikon EAP-in, i cili i përkrah një numër të protokolleve të autentifikimit siç është TLS (Transport Layer Security), MD5, TTLS dhe PEAP etj. për të cilët do të bëhet fjalë në vazhdim. Ndërkaq 802.1x/EAP siguron:

- identifikimin e bazuar në çertifikata dhe passworda.
- autentifikim të dyanshem në mes të klientit dhe serverit të autentifikimit
- i gjithë trafiku i cili nuk i takon 802.1x bllokohet përderisa shfrytëzuesi autentifikohet me sukses ne rrjet.

EAP metodat e autentifikimit janë:

EAP-MD5 është i bazuar në metodën e autentifikimt me password dhe nuk rekomandohet për rrjetat WLAN për shkak të autentifikimit të njëanshëm etj.

EAP-TLS përdoret në mjedise të bazuara në certifikata dhe ka siguri të lartë. Shkëmbyesi i mesazheve EAP-TLS siguron autentifikim të dyanshëm, negocim në lidhje me metodën e enkriptimit dhe shkëmbim të sigurt të çelësave në mes të shfrytëzuesit Wireless dhe rrjetës. EAP-TLS është mekanizëm, i cili siguron çelësa të enkriptuar dinamik për shfrytëzues dhe për sesione. Ky mekanizëm përmirëson sigurinë dhe tejkalon shumicën e dobësive të rrjetave Wireless LAN. Në Figurën 5 është paraqitur metoda kur Wireless shfrytëzuesi autentifikohet duke përdorur EAP-TLS. Dhe nevojiten dy çertifikata digjitale, njëra në RADIUS Server (EAS) dhe tjetra në shfrytëzuesin Wireless. Duhet cekur se qasja në rrjetë është e ndaluar derisa autentifikimi të bëhet me sukses dhe të jenë të vendosur çelësat dinamik Web [5]

EAP-TTLS and Protected EAP (PEAP) që te dyja janë metoda të autentifikimit si zgjerim i skemës se EAP-TLS, të cilat eliminojnë nevojën e përdorimit të certifikatave në anën e shfrytëzuesit, por sigurojnë autentifikim të dyanshëm. Autentifikimi bëhet në këtë mënyre:

Serverit ende i nevojitet një çertifikatë dhe kjo përdoret për autentifikim me shfrytëzuesin dhe krijimin e një tuneli të enkriptuar.

Klienti tani në mënyrë të sigurt autetifikohet në server duke përdorur njërën nga metodat p.sh password-at, ose edhe certifikatat mund të përdoren ende.
Protokolli 802.1x i pranon kërkesat nga EAP, i dërgon ato tek radius serveri dhe pret përgjigje. Në momentin kur e merr përgjigjen nga RADIUS server ai i lejon ose i ndalon qasjen ne rrjet.
Shfrytëzuesi e ka të instaluar paraprakisht çertfikatën e tij digjitale, sikurse edhe EAS-i. Shfrytëzuesi komunikon me EAS-it nëpërmjet AP.

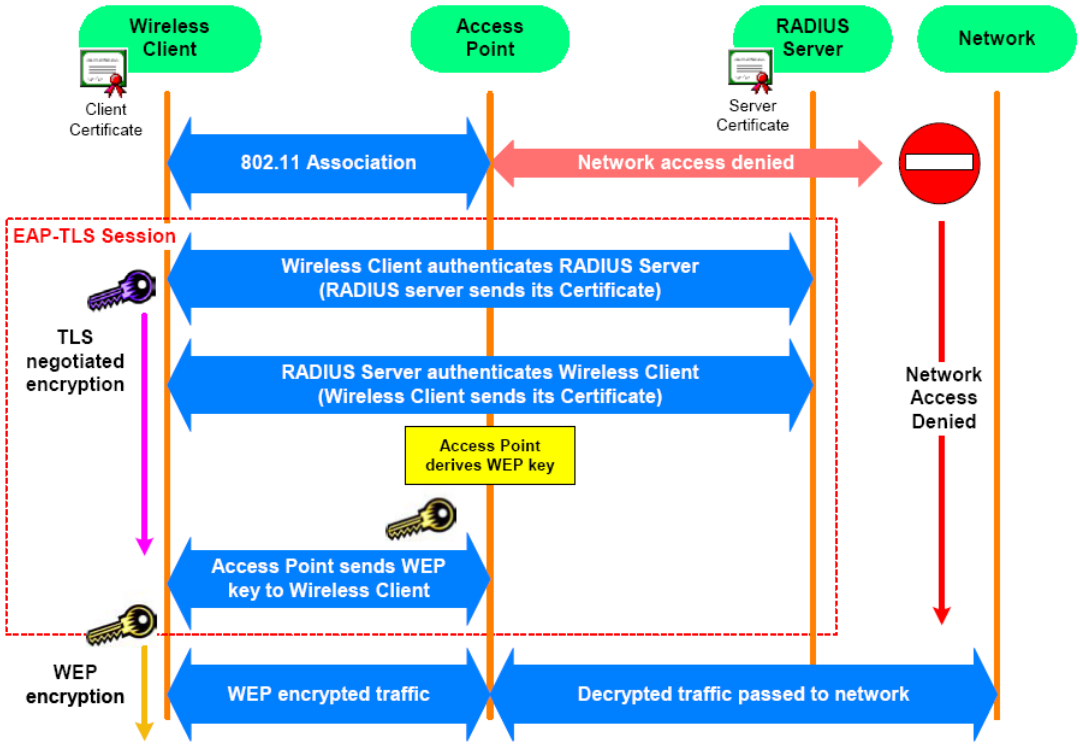

Figura 5 EAP-TLS autentifikimi [5]

5. WPA (Wi-Fi Protected Access)

Duke pare dobësitë e WEP, industritë e WLAN kanë reaguar kundër këtyre dobësive të WEP-it duke ofruar një zgjidhje me të fortë të sigurisë te quajtur WPA (Wi-Fi Protected Access).
WPA e ka rritur nivelin e mbrojtjes së të dhënave dhe qasjen e kontrolluar të sistemeve WLAN nëpërmjet standardeve bazë, ndëroperimit dhe specifikacioneve të sigurisë. WPA është i përcaktuar si një nën bashkësi e draft standardit 802.11i [2] .

WPA ka një numër përmirësimesh për dallim nga WEP, duke cekur dy ndryshimet më të mëdha dhe më të rëndësishme të cilat janë bërë në skemën e enkriptimit. WPA ka bërë zgjerimin e gjatësisë së vektorit të inicializimit nga 24 bita në 48 bita. Duke zvogëluar në masë të madhe mundësitë e dyfishimit të vektorit të inicializimit. Ky gjithashtu i shmanget mundësisë së përdorimit të ashtuquajturës “IV dobëta” të cilat janë shfrytëzuar nga WEP sulmuesit. Këta dy faktor janë implementur brenda një protokolli të ri të sigurisë të njohur si TKIP (Temporary Key

Integrity Protocol). TKIP pasi që përdorin çelësa të përkohshëm dinamik, të cilët që të gjithë nxirren nga master çelësa e që janë në maje të hierarkisë së TKIP çelësave. Ky superioritet mund të vërehet lehtë në krahasim me WEP master çelësat statik [9].
TKIP paketa përbehet prej tri elementeve:

1. Çelësa 128 bitësh që i ndahen edhe shfrytëzuesit edhe AP
2. MAC adresa e pajisjes së shfrytëzuesit
3. Vektori i Inicializimit 48 bitësh që përshkruan numrin e sekuencës së paketës.

Ne mënyrë që të jetë kompatibil me pajisje tjera TKI përdor algoritmin e njëjtë të enkriptimit (RC4) sikurse WEP-i.
Përmirësimet tjera që janë bërë në WPA përfshijnë:

- Përmirësim në MIC (Message Integrity Check) duke ulur mundësitë e ndërrimit të paketave në transit
- Përderisa çelësi WEP statik ende nevojitet të futet në secilën pajisje ky çelës nuk përdoret direkt, por kombinohet me MAC adresat e shfrytëzuesve dhe 48 bit IV[3] për ta gjeneruar çelësin që do ti enkriptoj të dhënat. Kështu që secila pajisje përdor keystream-in për ti enkriptuar të dhënat
- WPA gjithashtu i mundëson administartorit konfigurimin dhe ndryshimin e intervaleve të çelësave [4]

Përfundimi

Nga fillimi i këtij punimi e deri në fund të tij, jemi munduar që sadopak të japim informacione lidhur me WLAN Security. Synimi ka qenë që sa më shumë të jepen të dhëna rreth sigurisë së rrjetave Wireles LAN si komponente e domosdoshme dhe kruciale e kësaj lamie. Mbete edhe më tej që Institute të mëdha botërore siq është IEEE të punojnë në drejtim të standardizimit të protokolleve Wireless për tiu ofruar kompanive garantim të sigurt të shërbimeve, ndërsa shfrytëzuesve ofrime të shërbimeve të shpejta dhe të sigurta.

Ndërsa në vijim po japim 4 hapa që duhet të kihen parasysh domosdoshmërisht kur implementohet Wireless LAN

1. **Të aktivizohet siguria në shtresën fizike**, përderisa WEP i ka dobësitë e tij, TKIP specifikohet si pjesë e WPA dhe përmban nivel bazë të sigurisë. Ndërsa kur kombinohet me 801.11x atëherë ai përmban një nivel edhe më të fortë të sigurisë.
2. **Të mos shpërndahet ose përdoret default SSID,** duke e ndryshuar default SSID-në dhe duke e konfiguruar access point-in të mos transmetohet SSID
3. **Të përdoret 802.1X User Authentication,** kur konfigurohet Access pointi që ta mbështesë 802.11X, shfrytëzuesve nuk iu lejohet qasja në rrjet pa pasur kredibilitetet e duhura pra (user name/password ose certificates)
4. **Të implementohet Firewall-i personal,** edhe nëse ndonjë haker është i aftë që ti qaset rrjetës, Firewall-i personal do ti parandaloj ata në qasjen e fajllave apo në kompjuterin e shfrytëzuesit, i cili e përdor të njëjtën rrjet WLAN

[3] IV (Incicialsation Vecctor)

Referencat

[1] www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx?mfr=true

[2] Lasse Seppanen, skripta e dhënë në ligjerata

[3] IEEE 802.11 WLAN Security Performance Using Multiple Client

[4] IEEE 802.11-00/362

[5] Madge WLAN Security White paper.

[6] Testing on 801.11b networks, SANS Institute 2002

[7] Aaron E. Earle, Wireless Security Handbook, 2006 by Taylor & Francis Group, LLC

[8] S. Fluhrer, I.Mantin, A.Shamir

[9] http://ils.unc.edu/~bdoss/INLS187/WSecurity.htm

[10] http://www.wi-fiplanet.com/tutorials/article.php/1041171

[11] http://www.networkworld.com/research/2002/0506whatisit.html

[12] http://manageengine.adventnet.com/products/wifi-manager/weak-wep-iv-used.html