

Þráðlaus net

Sjálfstætt verkefni í Tölvuöryggi

Háskólinn í Reykjavík, Tölvunarfræðideild, Haustönn 2004.

Leiðbeinendur: Dr. Gísli Hjálmtýsson og Björn Brynjúlfsson.

Nemandi: Sigurjón Sveinsson.

1 Inngangur

Netsamskipti hafa lengi farið fram milli tölva og tölvukerfa. Til þess hafa verið notaðir netkaplar af ýmsum tegundum til að bera þau samskipti. En undanfarið hafa komið fram þráðlaus tölvusamskipti og útbreiðsla þeirra hefur verið ör og notkunin er orðin mjög algeng.

Í þessari greinagerð er ætlunin að taka fyrir ýmsar tegundir þráðlausra netsamskipta og lýsa þeim. Einnig verður ein tegund tekin sérstaklega fyrir og skoðaðir þeir öryggisgallar sem hafa komið fram í henni og hvernig hægt er að lagfæra þá galla.

2 Þráðlaus tölvusamskipti

Tölvusamskipti hafa lengi farið fram. Burðarvirki þeirra samskipta hafa lengstum verið netkaplar af ýmsum toga á borð við COAX, CAT3 og CAT5. Hægt er að byggja upp tölvunet með því að tengja þær allar saman innbyrðis með ákveðnum reglum. Einn eiginleiki þessara samskipta er að engin tölva getur verið með í netinu án þess að tengjast því með kapli. Netsamskiptin haldast því innan netsins.

Þráðlaus net eru byggð upp á allt öðrum forsendum. Öll samskiptin fara fram með útvarpsbylgjum milli sendipunkts og þráðlauss netkorts tölvunnar. Þessar útvarpsbylgjur geta allir numið og það eina sem tölva þarf að uppfylla til að vera með í netinu, ef ekki eru notaðar aðrar ráðstafanir, er að vera nógu nálægt sendipunktinum til að nema útvarpsmerkin. Þessi samskipti eru því ekki háð föstum efnum sem burðarvirki heldur berast þau í allar áttir og eru óháð föstum efnum.

2.1 Þráðlaus net (WiFi 802.11)

IEEE (e. Institute of Electrical and Electronics Engineers) þróaði útfærslu á þráðlausum netum og kom fram með 802.11 staðalinn árið 1997. Í dag hefur þessi staðall þróast mikið og er orðinn samheiti fyrir þrjár mismunandi útgáfur af honum. Þessar útgáfur eru 802.11a, 802.11b og 802.11g. 802.11 staðallinn fyrir þráðlaus net er oft kallaður WiFi sem er stytting á ensku orðunum Wireless Fidelity.

2.1.1. 802.11b

Fyrstur af WiFi stöðlunum til að koma á markað og ná útbreiðslu var 802.11b. 802.11b er á tíðninni 2,4 GHz og getur flutt allt að 11 Mbps.

2.1.2. 802.11a

802.11a kom á markað næst á eftir 802.11b. 802.11a er á tíðninni 5 GHz og getur flutt allt að 54 Mbps.

2.1.3. 802.11g

802.11g er blanda af *a* og *b* vegna þess að 802.11g er á tíðninni 2,4 GHz (eins og 802.11b) og flutningsgetan er allt að 54 Mbps (eins og 802.11a). 802.11g hefur því sama hraða og *a* en er á sömu bylgjulengd og *b*.

2.1.4. 802.11i

Eftir að 802.11 staðallinn kom fram komu í ljós margir gallar í honum er varða gagnaöryggi og aðgangsstýringar. IEEE áttaði sig á þessu fljótlega og setti af stað þróunarvinnu til þess að laga þessa galla. Í júní 2004 kom IEEE fram með nýjan staðal 802.11i sem felur í sér margar endurbætur í auðkenningu, lykrameðhöndlun og dulritun. Má þar nefna TKIP (e. Temporal Key Integrity Protocol) og CCMP (e. Counter-Mode/CBC-MAC Protocol).

2.2 Bluetooth

Bluetooth er práðlaus tækni sem snýr að samskiptum milli tækja. Það er hægt að láta hvaða tæki sem er tengjast nánast hvaða tæki sem er með Bluetooth og tæki á borð við mýs, lyklaborð, farsíma og lófátölvur nýta sér þessa tækni. Bluetooth var þróað af hóp er kallaði sig Bluetooth Special Interest Group (SIG) og voru þau samtök stofnuð í september 1998 af Ericsson, Nokia, Intel, IBM og Toshiba. Síðan þá hafa nær öll stærstu fyrirtækin á fjarskipta og tæknimarkaðinum gengið í þessi samtök og má þar nefna fyrirtæki á borð við Microsoft, 3Com, Motorola, Sony og mörg fleiri.

Bluetooth notar útvarpsbylgjur á tíðnisviðinu 2,4 GHz sem reyndar er sama tíðnisvið og örbylgjuofnar. Þetta tíðnisvið var tekið frá skv. alþjóðlegu samkomulagi til að nota í iðnaðartæki, hjúkruntæki og rannsóknartæki [6]. Bluetooth hefur yfirleitt ekki mikla drægni, um 10 metra, en hægt er að auka drægnina upp í 100 metra.

2.3 WiMax

WiMAX er nýleg práðlaus tækni sem var þróuð af samtökum sem kalla sig WiMAX Forum og samanstendur af mörgum leiðandi fyrirtækjum á fjarskipta og tæknimarkaðinum á borð við Motorola, AT&T, Cisco Systems, Dell, Intel Corporation og Fujitsu. WiMax byggir á IEEE 802.16 staðlinum og notar mjög breitt tíðnisvið, frá 2 til 66 GHz. Einnig er þessi staðall mjög langdrægur og getur flutt gögn allt að 50 km (með háum útvarpsmóstrum og öðrum skilyrðum) og gagnahraðinn getur farið upp í allt að 70 Mbps.

3 Öryggisgallar í útfærslum WiFi 802.11

Það er grundvallarmunur á práðlausum tölvusamskiptum og tölvusamskiptum á staðarnetum með netkapal. Ef tölvur eru ekki tengdar beint við netkaplana fara engin samskipti fram. Því er öðruvísi farið með práðlausu netin. Öll samskipti milli sendipunkta og práðlausra jaðartækja fara fram með útvarpsbylgjum og allir þeir sem eru nógu nálægt sendipunktunum eða jaðartækjunum til að geta numið þær útvarpsbylgjur geta hlustað á þau samskipti og tekið þátt. Það er nokkuð einfalt mál að hlusta á þessi samskipti og reynslan hefur sýnt að vegna alvarlegra galla í öryggisstöðlum í 802.11 staðlinum er ekki hægt að líta á WiFi net sem örugg.

3.1 WEP

Til að stýra aðgangi að þráðlausum netum, og þannig sjá til þess að óviðkomandi aðilar gætu ekki komist inn á lokuð net og til að fela gagnaflæði innan lokaðs þráðlauss nets, kom IEEE fram með svokallaðan WEP (e. Wireless Equivalent Privacy) öryggisstaðal. WEP átti að tryggja þrjá þætti í þráðlausum netum, sem eru:

1. **Trúnaður:** Helsta hlutverk og markmið WEP er að tryggja það að óviðkomandi aðilar geti ekki hlustað á samskiptin og komist að því hver þau eru. Sem sagt, að koma í veg fyrir hleranir.
2. **Aðgangsstýringar:** Annað hlutverk og markmið WEP er að tryggja aðgangsstýringar að þráðlausum netum. Að sjá til þess að óviðkomandi aðilar geti ekki notað þráðlaus net að vild.
3. **Gagnaheilindi:** Þriðja hlutverk og markmið WEP er að sjá til þess að þriðji aðili geti ekki breytt þeim gögnum sem send eru innan þráðlauss nets.

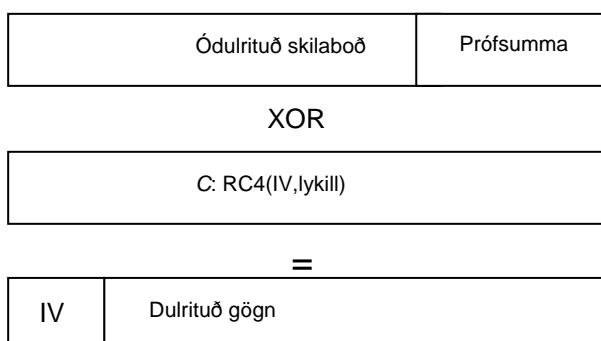
Ekkert af ofangreindum markmiðum hefur náðst og því er ekki hægt að segja að WEP geti sinnt þessum hlutverkum svo vel sé.

3.1.1. Hvernig virkar WEP?

WEP framfylgir trúnaði með því að nota strauma dulritun (e. stream cypher) sem kölluð er RC4. RC4 er einnig þekkt sem "Rivest Cipher 4" í höfuðið á höfundu RC4, prófessor Ronald L. Rivest í MIT háskólanum sem m.a. hefur hlotið hin eftirsóttu Turing verðlaun.

Til að dulrita pakka er notaður leynilykill (e. secret key), svokallaður WEP lykill. Þessi lykill er geymdur í hverjum þráðlausum sendipunkti sem og hjá þeim sem hefur aðgang að netinu, notandanum, og er einungis gefinn þeim sem eiga að hafa aðgang að þráðlausa netinu.

Byrjað er á því að reikna 32 bita prófsummu (e. checksum) af gögnunum sem á að senda. Prófsummunnunni er skeytt aftan á pakkann. Síðan er búinn til svokallaður IV bitastrengur (e. initialization vector) sem er 24 bitar. Með honum og leynilyklinum býr RC4 til annan bitastreng C. Sá bitastrengur er XOR-aður við ódulritaða strenginn og út úr því kemur dulritaður strengur. IV er skeytt framan á þann streng ódulritað og þá er pakkinn tilbúinn fyrir sendingu.



Á móttökustað er ferlinu snúið við, þ.e. móttakandi notar sama lykil og IV til að búa til C með RC4. C er XOR-aður við dulritaða strenginn og út úr því kemur ódulritaði strengurinn ásamt prófsummunnunni.

Móttakandi reiknar prófsummuna aftur og ber saman við þá prófsummu sem kom með pakkanum. Ef prófsumman er sú sama þýðir það að pakkanum hefur ekki verið breytt í sendingunni.

3.1.2. Fýsilegar árásir á WEP

Til að geta hafið árásir á dulrituð samskipti er það grundvallaratriði að geta komist yfir þau gögn sem þarf að dulráða. Þó svo að samskipti á þráðlausum netum fari fram með útvarpsbylgjum þarf samt sem áður að vita hvaða tækjabúnað þarf að hafa til að hlusta á þessi samskipti. Einnig þarf sá sem vill gera árás á þessi net að skilja vel hvernig þau samskipti eru uppbyggð og það getur tekið nokkurn tíma að ráða þessi samskipti. Þegar hakkari hefur komist yfir nægar upplýsingar til að geta hafið sjálfar árasina er nauðsynlegt að hafa rétt tæki og slík tæki geta verið dýr [2].

En þó svo að það geti verið erfitt nema fyrir helstu sérfræðinga að brjótast inn á þráðlaus net má ekki túlka það sem svo að það sé hægt að líta fram hjá þessari hættu. Því slík túlkun verndar þráðlaus net ekki gegn þeim sem hafa einbeittan brotavilja og góð úrræði til að framkvæma slíkar árásir. Slík túlkun væri sérlega hættuleg fyrir stórfyrirtæki sem þurfa að vernda dýrmætar upplýsingar því iðnaðarnjósnir geta verið mjög batasamar. Þessu til viðbótar hefur vélbúnaður, sem nothæfur í slíkar árásir, orðið aðgengilegri. Eru það aðallega netkort sem hægt er að kaupa og svo breyta í slíkum tilgangi.

3.2 Öryggisgallar í WEP

Fljótlega eftir að WEP staðallinn var gefinn út komu í ljós alvarlegir hnökrar á staðlinum. Rannsóknaraðilar í Berkeley háskólanum og og Zero-Knowledge Systems gáfu út rannsóknarniðurstöður sínar sem leiddu í ljós vandamál við IV endurnotkun. Þeir sýndu fram á það að öll möguleg IV gildi á einum nethnúti gætu klárast nokkuð fljótt [7]. Þessi galli gat orðið til þess að tölvuþrjótur gat fundið tvo pakka sem voru dulritaðir með sama bitastreng. Þessi galli gerði tölvuþrjóti kleyft að ekki einungis dulráða einn dulritaðan pakka heldur einnig að senda frá sér dulritaða pakka, breyta gögnum og beina gögnum til ákveðis IP vistfangs. Tölvuþrjóturinn getur einnig búið til gagnagrunn yfir öll IV gildin og bitastrengi leidda út frá þeim og þar með dulráðið allar þráðlausar gagnasendingar innan þráðlauss nets [4]. Á þeim tíma er þetta kom í ljós var ekki auðvelt að nýta sér þessa veikleika en það var bara tímaspursmál hvenær auðvelt yrði að misnota þennan grundvallarveikleika.

3.2.1. Endursending IV

IV bitastrengurinn er sendur óbrennlaður til móttakanda með hverjum pakka, í svokölluðum haus pakkans, svo að móttakandinn viti með hverju eigi að dulráða gögnin, auk leynilykilsins. En IV gildið hefur takmarkaða lengd því WEP staðallinn skilgreinir hann með 24 bita hámark. WEP staðallinn mælir einnig með að nota skuli IV sem breytist milli pakka en segir ekki til um hvernig. Sú útfærsla fer fram hjá hverjum framleiðanda fyrir sig. Þannig eru sumar útfærslur þannig að IV er alltaf núllstíllt við upphaf hverjar tengingar.

Þetta þýðir að í tengingum milli aðila á þráðlausu neti, þar sem IV gildið byrjar á fyrirfram ákveðnu gildi, t.d. 0, og er hækkað um 1 við hvern pakka, geta bara verið sendir 2^{24} (16.777.216) pakkar með einkvæmt IV. Eftir það verða endurtekningar í IV gildum sérstaklega þar sem ætla má að IV með lágum gildum séu tíð og mikið notuð.

Ef IV eru tilviljunarkennd gildi má búast við endurtekningu í IV eftir um 5000 pakka vegna svokallaðrar afmælisdaga þversagnar (e. birthday paradox) [4].

3.2.2. Veikleiki í KSA (Key Scheduling Algorithm)

Árið 2001 kom fram önnur rannsókn sem sýndi fram á enn verri veikleika í WEP en þann er kom fram í rannsókninni í Berkeley. Fluhrer, Mantin og Shamir (FMA) birtu niðurstöður rannsókna sinna í rannsóknargreinargerðinni "Weaknesses in the Key Scheduling Algorithm of RC4". Greinargerðin sýndi fram á tvo alvarlega galla í svokölluðum Key Scheduling Algorithm (KSA sem sér um að umræða bitum í dulritun eftir ákveðnu algrími) á mjög flókinn og stærðfræðilegan hátt.

Fyrri veikleikinn snéri að úrtaki KSA þar sem rannsóknaraðilarnir komust að því að lítill hluti leynilykilsins ákvarðaði stóran hluta af upphafsúrtaki KSA. Seinni veikleikinn, og sá alvarlegri, snérist um það að hægt er að brjóta leynilykilinn, komast að því hver hann er, á nokkuð auðveldan máta með því að fylgjast með gagnastráminum án þess að þurfa IV endurtekningar, sem minnst var á hér fyrir ofan. Fram að þessu hafði IV endurtekning og of fáir IV bitar verið talin aðalgalli WEP. Í þessari nýju uppgötvun kom fram að ekki einungis var þessi hönnunargalli í þeim WEP útfærslum sem eru í notkun í dag heldur einnig í arftaka WEP sem þá var á dagskrá, WEP2. FMA komust einnig að því að leynilykillinn sjálfur og IV stærðin breyttu litlu um þann tíma sem tók að brjóta lykilinn sem og að tíminn til þess að brjóta lykil óx línulega með stærð lykilsins í stað þess að vaxa veldislega [3].

Ákveðinn x fjöldi bita getur ákvarðað y marga bita í KSA úrtaki. Þetta gerist í mengi KSA bitastrengja sem hægt er að kalla R . Með því að skoða x bitana og bera þá saman við IV gildin, sem eru send ódulrituð, kemur stærri og stærri hluti leynilykilsins í ljós eftir því sem þetta er gert oftar. Eina skilyrðið er að hafa nógu stórt R mengi. Eftir því sem leynilykillinn sjálfur er lengri þarf einungis stærra R mengi og tíminn til að finna lykilinn vex línulega [10].

FMA settu niðurstöðu rannsókna sinna fram á fræðilegan máta og brutu aldrei lyklna í raunverulegu, práðlausu neti. En það leið ekki að löngu þar til einhverjir aðilar gerður það. Rannsóknarstofa AT&T í Bandaríkjunum og aðilar hjá Rice University notuðu fræðilega framsetningu FMA til að forrita lausn sem braut WEP lykla og dulréd dulritaða pakka og þar með staðfestu og sannreyndu fræðilega framsetningu FMA á veikleika WEP. AT&T og Rice University birtu aldrei upprunakóða lausnar sinnar en það leið ekki að löngu þar til aðrir aðilar höfðu útfært lausnir sem nýttu sama veikleika. AirSnort og WEPCrack eru forrit sem komu fljótlega fram og keyra á Linux. Þessi forrit þurfa ekki mikið gagnamagn til að brjóta WEP lykla, frá 100 MB til 1 GB.

3.2.3. Ný forrit fyrir hakkara gera WEP staðalinn algerlega ónýtan

6. ágúst 2004, á spjallþræðinum netstumbler.org, birti hakkari, undir dulnefninu KoreK, kóða og algrím sem braut WEP lykla á nýjan máta og á stuttum tíma [13]. Franskur hakkari að nafni Christophe Devine notaði þetta nýja algrím og bjó til forritið "aircrack" sem braut 128 bita WEP lykla á stuttum tíma, jafnvel aðeins á 5 sekúndum [16]. Greinarhöfundur [16] gerði tilraun með þetta forrit ásamt nokkrum öðrum og keyrði það með gögnum sem innihéldu WEP pakka, mismunandi marga. Niðurstöðurnar sýndu svo ekki var um að villast að WEP lykillinn sem öryggisstaðall er gersamlega ónýtur (sjá töflu).

Tími í sekúndum sem tók að brjóta 128 bita random WEP lykil.

Packets	Weak IVs	Unique IVs	aircrack	aircrack (4)	AirSnort	WepLab	WepLab	WEPCrack	dwepcrack
23.457.438	8.560	16.775.533	Failed	245	92	Failed	244	Failed	Error
21.016.149	1.807	16.775.167	Failed	249	41	Failed	247	Failed	Failed
19.584.364	9.340	16.275.925	Failed	230	114	Failed	229	Failed	Failed
15.690.079	8.694	12.860.342	Failed	184	90	Failed	179	Failed	Error
15.628.308	5.505	12.361.369	Failed	176	70	Failed	174	Failed	Failed
11.743.639	8.473	11.743.639	Failed	154	69	Failed	153	Failed	Error
11.739.339	3.037	11.693.841	Failed	150	Failed	Failed	151	Failed	Failed
7.829.104	1.001	5.031.233	Failed	74	Failed	Failed	77	Failed	Error
7.799.213	5.225	7.779.299	Failed	87	37	Failed	101	Failed	Failed
4.175.159	1.554	4.069.824	52	51	Failed	Failed	54	Failed	Failed
3.914.568	767	3.914.568	Failed	Failed	Failed	Failed	Failed	Failed	Error
3.914.553	3.958	3.914.553	48	49	Failed	Failed	56	Failed	Error
3.884.657	1.490	3.864.743	48	46	Failed	Failed	52	Failed	Failed
978.652	986	978.652	Failed	Failed	Failed	Failed	11	Failed	Error
978.633	371	978.633	Failed	12	Failed	Failed	13	Failed	Error
977.219	264	974.902	Failed	9	Failed	Failed	13	Failed	Failed
684.992	143	684.992	8	8	Failed	Failed	11	Failed	Error
683.605	238	681.288	Failed	18	Failed	Failed	13	Failed	Failed
587.184	117	587.184	Failed	27	Failed	Failed	Long	Failed	Error
489.293	103	489.293	8	7	Failed	5	5	Failed	Error
489.286	115	489.286	15	16.116	Failed	Failed	Long	Failed	Error
391.465	78	391.465	5	13	Failed	Failed	Long	Failed	Error
391.433	78	391.433	Failed	6	Failed	Failed	6	Failed	Error
293.596	65	293.596	Failed	5	Failed	Failed	Long	Failed	Error
293.579	65	293.579	Failed	Failed	Failed	Failed	Failed	Failed	Error

[16]

3.3 Veikleiki í aðgangsstýringum

Um svipað leiti og veikleikar WEP voru að koma í ljós voru aðrir veikleikar 802.11 staðalsins að uppgötvast. Rannsóknaraðilar við Maryland Háskóla (University of Maryland) uppgötvuðu nokkra veikleika við aðgangsstýringar sem algengir práðlausir hnútar notuðu.

Venjulega hafa práðlausir hnútar fleiri en eina aðferð til aðgangsstýringar eins og SSID (e. Service Set Identifier), MAC viðfangssíu og fyrrgreindann WEP lykil.

3.3.1. SSID

SSID snýst um það að práðlaust net ber nafn. Þetta er hægt að nota þannig að práðlausir sendipunktara eru stilltir á þann veg að þeir varpa ekki út nafninu heldur þarf að vita þetta nafn til að komast inn á netið. Og þar sem að WEP er einungis valkostur á sendipunktum frá ýmsum framleiðendum er SSID eina virka aðgangsstýringin ef WEP er ekki virkjað.

Í stórborgum hafa margir stundað það að keyra um og leita að práðlausum netum (e. war driving) þar sem auðvelt er að finna SSID netanna með réttum loftnetum og hugbúnaði á borð við Network Stumbler sem hægt er að ná í án endurgjalds. Kevin Poulsen skrifaði grein 2001 þar sem Peter Shipley, ráðgjafi í tölvuöryggi, ók um San Francisco borg, með loftnet tengt við práðlaust netkort og sérstakan hugbúnað. Þeir keyrðu um miðborgina og á einum klukkutíma fundu 80 práðlaus net fyrirtækja þar sem SSID var eina aðgangsstýringin, WEP var óvirkt [9]. Þessi veikleiki getur boðið upp á það að hakkarar komist nógu nálægt netunum, t.d. með því að leggja bílum sínum við byggingar fyrirtækja, til að hafa aðgang að netinu, brjóta sér leið inn á netið og ráðast þannig á netið úr öruggri

fjarlægð eða misnota það með niðrhali gagna. Menn hafa verið dæmdir í margra ára fangelsi í Bandaríkjunum einmitt fyrir slíkar árásir [12].

3.3.2. MAC vistfangasía

Enn ein leið til að stýra aðgangi er að hleypa ekki práðlausum netkortum hnúta inn á netið nema með ákveðnum MAC vistföngum. Listi samþykktra vistfanga fyrir práðlaust net er þá geymdur í hverjum og einum práðlausum aðgangshnúti. Það eru nokkur vandamál sem tengjast þessari aðferð við auðkenningu. Í fyrsta lagi er verið að auðkenna tæki gagnvart netinu en ekki notanda. Ef netkortið kemst í hendur óprúttna aðila er auðvelt fyrir þá að komast inn á netið ef engrar annarrar auðkenningar er krafist. Aðilar innan Maryland Háskóla komust að því í rannsóknum sínum að þetta væri ekki heldur trygg leið til að stýra aðgangi því að MAC vistföng væri auðvelt að finna með hugbúnaði, svokölluðum “packet sniffer” [8] og þannig komast að því hvaða MAC vistföng komast á netið. Ef MAC vistfangið er vitað væri hægt að breyta MAC vistfanginu, í netspjöldum í stýrikerfinu eða með forritum á borð við SMAC frá KLC og a-Mac Address Change frá Paqtool, til að nýta það sem auðkenningu inn á netið.

3.4 Öryggisþættir ekki í leiðbeiningum til kaupenda

Práðlaus net verða sífellt vinsælli á heimilum ekki síður en í fyrirtækjum. Fjarskiptafyrirtækin keppast um að koma fram með betri og betri tilboð með ADSL nettenginum og oft fylgir práðlaus neghnútur með í kaupunum. Verslanir með tölvubúnað auglýsa ódýran práðlausan búnað og mikið er selt. En svo virðist sem öryggismál séu ekki ofarlega í huga þeirra sem selja og framleiða þennan búnað.

Þegar kaupandinn fær búnaðinn í hendurnar fylgja yfirleitt góðar leiðbeiningar um það hvernig á að setja þennan búnað upp þannig að hann fari að virka. En leiðbeiningarnar fara mjög oft ekki lengra en það. Oft ráðleggja þær ekki notendum að nota WEP lykilinn, fela SSID sendipunktsins, nota MAC viðfangs síuna né heldur að nota nýrri og fullkomnari öryggisráðstafanir. Einu leiðbeiningarnar sem snúa að öryggisþáttum einblína á það að skipta um það lykilorð sem þarf að gefa upp til að geta breytt stillingum á nethnútnum.

En þegar þessir nethnútar eru settir upp fyrst eru ofantaldir öryggisþættir ekki virkir og práðlausu netin því galopinn öllum þeim sem hafa práðlaus netkort í tölvum sínum og eru nógu nálægt til að komast í samband við netin. SSID er ekki falið og því sést það þegar stýrikerfið leitar eftir netum, enginn WEP lykill er notaður og því þarf ekki að setja neitt lykilorð fyrir hann og MAC sían ekki notuð og því geta öll netkort tengst netinu.

4 Úrlausnir fyrir WiFi

4.1 WPA (Wi-Fi Protected Access)

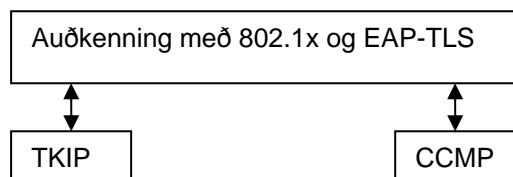
Eftir afhroð WEP ákvað Wi-Fi Alliance, sem eru samtök hagsmunaaðila í práðlausum samskiptum, í samvinnu við IEEE að bæta öryggismál Wi-Fi og 2003 kom fram með lausn til að bæta öryggi práðlausra neta. Þessi lausn var kölluð WPA (Wi-Fi Protected Access) og var hugsuð sem tímabundin lausn á meðan nýr staðall fyrir práðlaus net var í smíðum.

WPA notar 802.1x auðkenningarþjón til að dreifa mismunandi lykllum til notenda sem tengjast netinu. WPA getur þó áfram notað einn miðlægan lykil á borð við þann sem WEP notar í dag þó sú leið sé mun öruggari. Gögnin eru dulrituð með RC4 algríminu, eins og WEP, en með 48 bita IV og með 128 bita lykli. En helsta umbótin er þó TKIP (e. Temporal Key Integrity Protocol) sem breytir þeim lykllum sem notaðir eru á kviklegan máta og dulritar IV gildið. Með því að blanda saman dulrituðu IV sem hefur helmingi fleiri bita og TKIP er komin lausn á þeim vandamálum sem gera WEP jafn ótryggan og hann hefur reynst vera [11].

Með þessu þurfa notendur að auðkenna sig gagnvart netinu ásamt því að þráðlausu samskiptin verða mun öruggari og heilindi gagnanna betur tryggð. Til viðbótar eru heilindi betri í WPA með tilkomu MIC tætifalls. MIC tætifallið reiknar 32 bita prófsummu af öllum pakkanum, ekki einungis gögnunum í honum. MIC tætifallið kemur sem viðbót við fyrra tætifallið sem notað hefur verið.

4.2 802.11i

Eftir að í ljós kom að WEP lykillinn í þráðlausum netum reyndist hafa alvarlega hönnunargalla fór Wi-Fi Alliance að hanna nýjan staðal fyrir þráðlaus net. Í júní 2004 var 802.11i staðallinn samþykktur af IEEE en Wi-Fi Alliance kallar hann WPA2. Þessi staðall er framhald af WPA með nokkrum breytingum. Það má líta á hann sem þrískiptann.



4.2.1. Auðkenning með EAP-TLS

Auðkenning við þráðlausa netið fer fram með EAP-TLS (e. Extensible Authentication Protocol - Transport Layer Security) [RFC-2716]. EAP er auðkenningar algrím og auðkennir notandann gagnvart netinu og netið gagnvart notandanum. Hægt er að nota ýmsar aðferðir til að halda utan um gögnin fyrir auðkenningar eins og Kerberos, Public Key, One Time Passwords og RADIUS. EAS sér um að koma þeim milli nethnútsins og notandans. EAP sér einnig um að skiptast á 128 bita dreifilyklum (e. key management) sem notaðir eru til að dulrita samskiptin. TLS sér um að dulræða samskiptin við auðkenninguna.

Þessi aðferð við auðkenningu er mjög umfangsmikil og krefst aðkomu annarra kerfa. Því er líklegra að EAP-TLS verði notuð í fyrirtækjum frekar en á heimilum því fyrirtæki hafa frekar yfir að ráða þeim tölvukerfum og auðlindum sem til þarf.

4.2.2. Dulritun með CCMP og TKIP

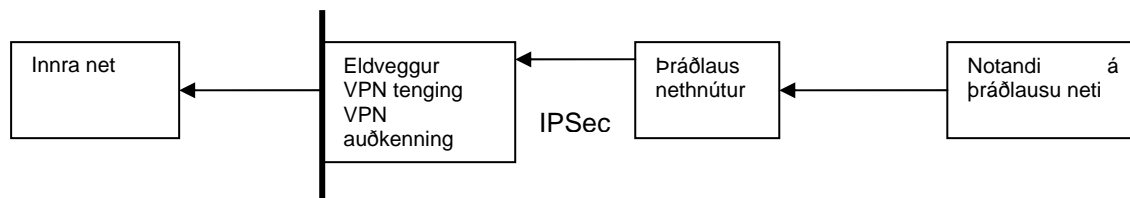
Í stað þess að nota RC4 og tætiföll til að dulrita gögn og tryggja heilindi gagna notar 802.11i algrím sem byggir á AES (Advanced Encryption Standard) dulritunaralgríminu. Þessi nýji staðall hefur verið kallaður CCMP sem stendur fyrir "Counter mode/CBC-MAC Protocol" og er í raun sambland af tveim þáttum. Counter mode er algrím fyrir dulritun og kemur úr AES. CBC-MAC stendur fyrir "Cipher Block Chaining-Message Authentication Code" og sér um gagnaheilindi.

CCMP notar 128 bita dreifilykla til að dulrita gögnin. Til að vel sé þarf netkort hvernar tölvu að vera með sérstakan örgjörva til að dulrita og dulráða gögnin þar sem AES er mjög óhentugt að útfæra í hugbúnaði og frekar útfært í vélbúnaði.

TKIP, sem lýst var í kafla 4.1 WPA (*Wi-Fi Protected Access*) er valfrjálst í 802.11i þannig að framleiðendur geta notað TKIP en það er ekki skilda að nota það. Kosturinn við að hafa TKIP með er að sá staðall er hentugri til að nota á heimilum.

4.3 VPN

Það er hægt að bæta auðkenningu og gagnaheilindi 802.11 a og b (WEP) með því að setja upp eldvegg með VPN (e. Virtual Private Network) milli práðlausu hnútanna og innra staðarnets. Þannig er práðlausu netið ekki beintengt við innra netið með öllum þeim öryggishættum sem því fylgir heldur þurfa samskiptin að fara í gegnum mun sterkari dulritun í VPN eins og IPSec og notendur netsins þurfa að auðkenna sig gagnvart VPN tengingunni með notendanafni og lykilorði.



Með þessu eru sett sterk öryggisskil á milli staðarnets og práðlauss nets og öryggi staðarnetsins mun betra en með núverandi ráðstöfunum práðlausra neta.

5 Öryggisgallar í útfærslum bluetooth

Fram hafa komið gallar í bluetooth sem snúast í aðalatriðum um þrennt:

1. Hægt er að nálgast trúnaðarupplýsingar á GSM sínum með bluetooth á nafnlausan máta og án vitneskju eiganda þeirra. Í þessum upplýsingum eru símaskrá notandans, IMEI símans og dagbók. (SNARF)
2. Allt minni sumra GSM síma er aðgengilegt með tækjum sem hafa áður verið með trausta tengingu við símann en síðan verið tekin úr því mengi tækja sem geta tengst símanum. Þau gögn sem eru aðgengileg á þennan máta eru símaskráin, dagbókin, textaskilaboð og myndir. (BACKDOOR)
3. AT skipanir sumra síma eru aðgengilegar gegnum bluetooth. Þar með er opinn aðgangur að mikilvægum aðgerðum símans eins og t.d. hringingar, SMS skilaboð og gögn í minni. (BLUEBUG)
4. Bluejacking er ekkert annað en tilraunir til að blekkja símanotendur til að samþykkja tengingar milli tækja með bluetooth. Send er beiðni um tengingu og er beiðnin dulbúin sem textaskilaboð. Textinn getur verið hvetjandi fyrir notandan til að samþykkja tenginguna. Ef hann samþykkir tenginguna er hægt að nota þá tengingu til að komast í gögn á símanum.

5.1 SNARF

Það er mögulegt á sumum tegundum af símum að tengjast þeim án þess að eigandi þeirra síma verði þess var. Með þessum aðgangi er hægt að nálgast gögn á símanum í minni á borð við símaskrá símans, dagbók og einkvæmt verksmiðju númer símans (IMEI, e. International Mobile Equipment Identity). Með því að ná IMEI númeri símans, sem er einkvæmt númer sem einkennir símann gagnvart símakerfum, og misnota það til þess að klóna símann, eða númer hans, á ólöglegan máta [5].

Þessi árás er undir venjulegum kringumstæðum aðeins möguleg ef síminn er í sýnilegum ham (e. visible mode) þannig að önnur tæki "sjái" hann. En það eru til forrit, aðgengileg á internetinu, sem fara framhjá þeim ráðstöfunum. Þeirra á meðal eru bluesniff, btscanner og redfang.

Adam Laurie, starfsmaður A.L. Digital Ltd. notaði SNARF til að komast í síma nokkurra þingmanna á breska þinginu og gat náð þannig í viðkvæmar upplýsingar (þó hann gerði það ekki) og olli þessi uppgötvun því að öll bluetooth tæki voru bönnuð með öllu í breska þinginu [14].

5.2 BLUEBUG

BLUEBUG er öryggisgalli sem er í sumum GSM símum er eru með bluetooth. Með BLUEBUG árás er hægt að nálgast gögn á símanum á borð við símaskrá eigandans en einnig er hægt að senda AT skipanir til símans. AT skipanir eru skipanasett sem síminn notar til að framkvæma langflestar aðgerðir eins og að hringja, senda SMS skilaboð, lesa SMS skilaboð, lesa úr gögnum símans, tengjast internetinu með GPRS og margt annað.

5.3 BACKDOOR

BACKDOOR árásin snýst um að koma á nokkurs konar trausti milli síma með bluetooth en einnig að sjá til þess að sú tenging, sem notuð er til árárarinnar, sé sýnileg á símanum sem fyrir henni verður. Til þess að verða þess var verður fórnarlambið að vera að horfa á símann þegar tengingin verður til.

Með því að ná þessari tengingu er hægt að nálgast viðkvæmar upplýsingar á símanum auk þess að hægt er að nálgast mikilvægar þjónustur sem síminn veitir á borð við WAP og GPRS.

5.4 Bluejacking

Tilgangur bluetooth er að tæki geti á auðveldan máta tengst öðrum tækjum á þráðlausan máta. Þessi tenging er í tveim skrefum og það fyrsta er þegar tæki *A* biður tæki *B* um að samþiggja tengingu og stofna traust á milli þeirra. Þegar fyrsta skrefið er tekið sendir tæki *A* nafn sitt til *B*. *B* fær skilaboð um að *A* vilji tengjast sér og sér nafn *A*. Þetta nafn getur verið mjög langt, allt að 248 stafir. Þar af leiðandi hefur fólk farið að nota sér þetta til að nota nöfn á tengingum sem eru skilaboð í eðli sínu. Dæmi um slíka tengingu væri t.d. að skýra hana "Hello, you just won \$1.000, press OK to collect the price!" og hefja tengingar með þessu.

Notkun á þessum möguleika á skeytasendingu hefur aukist mikið undanfarið. En aukningin veldur því að þetta verður sjálfsgðara og jafnvel geta framleiðendur minnst á þennan möguleika við markaðssetningu. Ef *B* samþykkir tenginguna því hún hefur gaman af vinningum getur *A* notað þá tengingu til að fá aðgang að gögnum *B* með ófyrirséðum afleiðingum.

5.5 Símar með bluetooth öryggisveilur

Eftirfarandi er tafla [15] yfir nokkra síma frá helstu framleiðendum GSM síma og hvort þeir séu veikir fyrir árásum á bluetooth búnað þeirra.

Framleiðandi	Model	Firmware Rev	BACKDOOR	SNARF sýnilegur	þegar SNARF EKKI sýnilegur	þegar	Galli
Ericsson	T68	20R1B, 20R2B013, 20R5C001	20R2A013, 20R2F004, ?	Já	Nei		Nei
Sony Ericsson	R520m	20R2G	?	Já	Nei		?
Sony Ericsson	T68i	20R1B, 20R2B013, 20R5C001	20R2A013, 20R2F004, ?	Já	?		?
Sony Ericsson	T610	20R1A081, 20R3C002, 20R4D001	20R1L013, 20R4C003, ?	Já	Nei		?
Sony Ericsson	T610	20R1A081	?	?	?		Já
Sony Ericsson	Z1010	?	?	Já	?		?
Sony Ericsson	Z600	20R2C007, 20R5B001	20R2F002, ?	Já	?		?
Nokia	6310	04.10, 04.20, 4.07, 4.80, 5.22, 5.50	?	Já	Já		?
Nokia	6310i	4.06, 4.07, 4.80, 5.10, 5.22, 5.50, 5.51	Nei	Já	Já		Já
Nokia	7650	?	Já	Nei (+)	?		Nei
Nokia	8910	?	?	Já	Já		?
Nokia	8910i	?	?	Já	Já		?
* Siemens	S55	?	Nei	Nei	Nei		Nei
* Siemens	SX1	?	Nei	Nei	Nei		Nei
Motorola	V600	?	Nei	Nei	Nei		Já
Motorola	V80	?	Nei	Nei	Nei		Já

5.6 Úrlausnir fyrir bluetooth

Til að koma í veg fyrir SNARF og BLUEBUG árásir eru ekki til í dag aðrar aðferðir en þær að slökkva á bluetooth búnaði símans og PDA tækjanna. Til að eyða út endanlega öllum eyddum tengingum við önnur tæki, og þar með koma í veg fyrir BACKDOOR árásir, þarf að endurstilla símann með verksmiðjustillingunum (e. factory settings). En með því er hætt á að önnur gögn á borð við símaskrá tapist. Til að koma í vef fyrir Bluejacking þarf bara að velja "nei" möguleikan er slíkar tengingar eru hafnar.

En best er að leita til framleiðenda símanna til að fá endanleg svör og endanlegar lausnir á þessu öryggisgöllum.

6 Lokaorð

Þróunin í práðlausum samskiptum er hröð og er það vel. Práðlaus tölvusamskipti eru í dag mjög útbreidd og fara vaxandi í tölum, sínum, lófatölum og mörgum jaðartækjum. Heimanet, þar sem langflest heimilistæki á heimilum og hýbýlum eru nettengd, eru einnig í hraðri þróun og margar lausnir þar eru práðlausar. En kapp er best með forsjá. Þessi samskiptamáti verður að vera hannaður frá byrjun með öryggi í huga. Ef framleiðendur og hagsmunaaðilar fara of geyst af stað með nýjar lausnir og staðla sem hafa öryggisgalla býður það upp á misnotkun. Gott dæmi um staðal þar sem öryggismál voru vanmetin og illa hönnuð er WEP staðallinn. Hann er svo slæmur að það er orðið formsatriði fyrir fólk með sæmilega þekkingu að brjóta WEP lykila á nokkrum mínútum, jafnvel undir mínútu í góðum skilyrðum. Ef öryggismál eru hunsuð getur það haft alvarlegar afleiðingar. Fyrir einstaklinga og sérstaklega fyrirtæki sem búa yfir viðkvæmum upplýsingum. Þar af leiðandi verða öryggisþættir práðlausra samskiptastaðla að vera vel útfærðir og vera eitt af forgangsaðilunum í samskiptastöðlum.

7 Heimildaskrá

- [1] Marshall Brain, How Stuff Works. *How WiFi Works*.
<http://computer.howstuffworks.com/wireless-network.htm>
- [2] Sean Convery, Darrin Miller, og Sri Sundaralingam, 2003. *Wireless LAN Security in Depth*.
<http://www.securitydocs.com/go/290>
- [3] Scott Fluhrer, Itsik Mantin, and Adi Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- [4] Nikita Borisov, Ian Goldberg, David Wagner, 2001. *Intercepting Mobile Communications: The Insecurity of 802.11* <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>
- [5] Martin Herfurt 2004, *Bluesnarfing @ CeBIT 2004*.
http://trifinite.org/Downloads/BlueSnarf_CeBIT2004.pdf
- [6] Curt Franklin. *How Bluetooth Works*. <http://electronics.howstuffworks.com/bluetooth.htm>
- [7] Nikita Borisov, Ian Goldberg, David Wagner, 2001. *Security of the WEP algorithm*
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- [8] William A. Arbaugh; Narendar Shankar og Y.C. Justin Wan, 2001. *Your Wireless Network has No Clothes*. <http://www.cs.umd.edu/~waa/wireless.pdf>
- [9] Kevin Poulsen, 2001. *War driving by the Bay* <http://www.securityfocus.com/news/192>
- [10] Scott Fluhrer, Itsik Mantin, and Adi Shamir, *Attacks on RC4 and WEP*.
http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/rc4_wep.ps
- [11] Wi-Fi Alliance, 2003. *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*
http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf
- [12] Kevin Poulsen 2004. *Long prison term for Lowe's wi-fi hacker*.
<http://securityfocus.com/news/10138>
- [13] KoreK (dulnefni á spjallþræði) 2004. *(Aircrack) Yet another WEP cracking tool for Linux*
<http://www.netstumbler.org/showpost.php?p=89692&postcount=22>
- [14] Annalee Newitz 2004. *They've Got Your Number ...*
http://www.wired.com/wired/archive/12.12/phreakers.html?tw=wn_tophead_5
- [15] Adam Laurie og Ben Laurie, The Bunker 2004. *Serious flaws in bluetooth security lead to disclosure of personal data*.
<http://www.thebunker.net/security/bluetooth.htm>
- [16] Michael Ossmann 2004. *WEP: Dead Again, Part 1*
<http://securityfocus.com/infocus/1814>