

# Säkerheten i Wlan

Peter Andersson  
peter@it-slav.net  
KTH Syd

1 december 2004

## Innehåll

<b>1</b>	<b>Inledning</b>	<b>3</b>
<b>2</b>	<b>Wlan, en introduktion</b>	<b>4</b>
2.1	Standarder . . . . .	4
2.2	Wlan topologier . . . . .	4
2.3	Wlan konfigurering . . . . .	4
2.4	Praktikaliteter . . . . .	5
<b>3</b>	<b>Hot och risker</b>	<b>6</b>
<b>4</b>	<b>Lösningar för att skydda sig</b>	<b>7</b>
4.1	Wep . . . . .	7
4.2	Starkare WEP . . . . .	8
4.3	WPA . . . . .	8
4.4	VPN . . . . .	9
4.5	Låsta MAC-adresser . . . . .	10
4.6	SSID . . . . .	11
<b>5</b>	<b>Attackmetoder</b>	<b>11</b>
5.1	Attack av WEP . . . . .	11
<b>6</b>	<b>Empiriskt test</b>	<b>12</b>
<b>7</b>	<b>Slutsatser</b>	<b>12</b>
<b>A</b>	<b>Referenser</b>	<b>13</b>
<b>B</b>	<b>Förkortningar, Ordlista</b>	<b>14</b>

## Figurer

1	Wlan med en central accesspunkt . . . . .	5
2	Wlan peer-to-peer . . . . .	5
3	VPN tunnel i WLAN . . . . .	10

## Tabeller

1	WLAN standarder . . . . .	4
2	Hastighetsjämförelse av symmetrisk krypering på en Pentium II . . . . .	10
3	Förinställd SSID . . . . .	11

# 1 Inledning

Wlan<sup>1</sup> är en teknik för att koppla ihop datorer utan att använda sladdar. Istället används radiokommunikation för att sända data mellan noderna. Det finns många fördelar med att kunna använda ett nätverk och dess resurser utan att behöva några sladdar, några av fördelarna är:

- enkel installation då man ansluter en Wlan-hub<sup>2</sup> på lämpligt ställe istället för att dra sladdar ifrån en punkt i huset till alla rum
- slipper trassel med sladdar
- får en mobil arbetsmiljö där man enkelt kan flytta sin dator med sig in i ett annat rum
- om man skall ansluta en ny nod behöver man inte ansluta dess nätverksuttag i ett korskopplings-skåp

Men det finns även nackdelar då man inte behöver fysiskt koppla in sig på nätet utan kan på avstånd genomföra diverse attacker mot nätet. Användningen av Wlan är allt ifrån hemmanätverk till stora företag, då kompetensnivån hos de som administrerar och konfigurerar näten i de olika miljöerna skiljer sig åt kan angripare använda olika metoder för att attackera näten. Några av dessa risker skall belysas i denna uppsats. Som vanligt när det gäller IT-säkerhet handlar det om att hitta en nivå av säkerhet som är lagom, d.v.s. kostnaden för att skydda sig skall stå i proportion till de skador en eventuell angripare<sup>3</sup> kan ställa till med.

Genomgående i texten används ordet hacker för att illustrera en illvillig person som använder sitt kunnande för att attackera olika typer av IT-system. Att använda ordet hacker kan vara kontroversiellt då den ursprungliga betydelsen är en person som är duktig på datorer. Tyvärr har denna betydelse förskjutits till att betyda något annat och i dag så används nästan uteslutande ordet hacker för att beskriva en person som använder en dator på ett otillbörligt sätt[1].

---

<sup>1</sup>Wireless Local Area Network

<sup>2</sup>Det finns många namn på den enhet där Wlan noderna kommunicerar mot, några är accesspunkt, centralenhet, basenhet, router m.fl.

<sup>3</sup>En angripare kan vara avsiktlig eller oavsiktlig

## 2 Wlan, en introduktion

Detta kapitel beskriver på ett övergripande sätt hur ett WLAN fungerar. Den absolut vanligaste teknologin för Wlan kallas 802.11 och brukar vara det man menar med Wlan. Genomgående för detta dokument är att med Wlan menas 802.11 om inte annat anges<sup>4</sup>.

### 2.1 Standarder

De WLAN standarder som finns i dagsläget[4] sammanfattas i tabell ??  
Bluetooth, HomeRF och HiperLAN är med som referens.

<i>Namn</i>	<i>Frekvens</i>	<i>Maxhastighet</i>	<i>Säkerhet</i>
IEEE 802.11 <sup>5</sup>	2,4 Ghz	2 Mbps	WEP eller WPA
IEEE 802.11a (Wi-Fi <sup>6</sup> )	5 Ghz	54 Mbps	WEP eller WPA
IEEE 802.11b (Wi-Fi)	2,4 Ghz	11 Mbps	WEP eller WPA
IEEE 802.11g (Wi-Fi)	2,4 Ghz	54 Mbps	WEP eller WPA
Bluetooth	2,45 Ghz	2 Mbps	PPTP <sup>7</sup> , SSL <sup>8</sup> eller VPN
HomeRF	2,4 Ghz	10 Mbps	56-bitars kryptering
HiperLAN/1	5 Ghz	20 Mbps	Sessionsbaserad och individuellt
HiperLAN/2	5 Ghz	54 Mbps	Stark kryptering som är sessionsbaserad

Tabell 1: WLAN standarder

### 2.2 Wlan topologier

Det finns två olika sätt att bygga upp sitt Wlan[2]. Det vanligaste är att man har en eller flera centrala accesspunkter där noderna ansluter sig mot, se fig 1. Den andra metoden att bygga upp sitt Wlan på är att använda peer-to-peer, även kallat Ad-Hoc, där noderna kommunicerar direkt med varandra, se fig 2. Peer-to-peer lämpar sig bäst för små nätverk t.ex. i ett konferansrum, SOHO<sup>9</sup> eller i en hemmamiljö.

### 2.3 Wlan konfigurering

För att kunna få noderna i Wlanet att kunna kommunicera med varandra behövs två komponenter:

<sup>4</sup>VAFAN HÄNDE MED ÖVRIGA FOTNOTER???

<sup>9</sup>Small Office Home Office



Figur 1: Wlan med en central accesspunkt



Figur 2: Wlan peer-to-peer

1. *Nätverksnamn*, alla Wlan har ett namn, för att identifiera nätverket. Detta namn kallas SSID<sup>10</sup>. Detta namn sätter den som installerar nätverket och namnet kan vara upp till 32 tecken långt och bestå av bokstäver och siffror. Om man vill ansluta till ett befintligt Wlan måste man konfigurera sin nod att använda korrekt SSID.
2. *Säkerhet*, 802.11 Wlan kan använda sig av flera tekniker för att skydda trafiken, WEP<sup>11</sup> är den vanligaste. Huvudanledningen till att WEP finns med i 802.11 standarden är att hindra obehöriga att avlyssna nätet[8] men WEP hindrar också mot att obehöriga använder nätet. På senare tid har en ny skyddsteknik utvecklats WPA<sup>12</sup> för att lösa de problem som WEP har. I den utrustning som säljs idag finns oftast stöd för både WEP och WPA.

## 2.4 Praktikaliteter

Wlan använder sig av två frekvenser för att kommunicera 2,4 GHz samt 5 GHz[3]. Då dessa frekvenser är relativt höga är antennernas placering viktig, dessutom kan olika föremål påverka hur radiovågorna transporteras.

<sup>10</sup>Service Set Identifier

<sup>11</sup>Wired equivalent privacy

<sup>12</sup>Wi-Fi Protected Access

Det är således vanskligt att gissa hur långt ett Wlan når. En tumregel är att ett WLAN räcker 100 meter inomhus och 300 meter utomhus.

### 3 Hot och risker

Wlan är ofta inte skyddade[5], även om nätverksadministratörerna använder sig av WEP. En undersökning i London visar att 94% av Wlan näten inte använder tillräckligt skydd mot attacker. För att genomföra en attack behöver förövaren inte någon avancerad utrustning utan det ända som behövs är en dator med ett Wlan kort och rätt programvara d.v.s. den som attackerar behöver inte någon dyr utrustning vilket medför att vem som helst med de rätta kunskaperna är potentiella hot. Om man har ett Wlan så är risken mycket stor att någon attackerat nätet. Den som utför en attack mot ett Wlan kan ha olika motiv såsom:

- *Utnyttja bandbredd.* Om någon i ett bostadshus skaffat sig ett Wlan och har detta anslutet till ett bredbandsnät kan grannarna också utnyttja detta för att utföra ärenden på internet såsom, eposta och surfa m.m. I folkmun kallat *fulsurfa*.
- *Utföra anonyma attacker på internet.* Om en illvillig person som vill utföra attacker på internet får tillgång till en bredbandsanslutet Wlan, kan denna utföra sin gärning totalt anonymt. Om någon försöker spåra vem som gjort internetattacken kommer ägaren av bredbandsanslutningen att vara den som pekas ut.
- *Snappa upp intressant information.* Om ägaren eller någon fulsurfare använder sitt Wlan för att utföra bankärenden eller köpa varor på internet kan kontonummer, PIN<sup>13</sup>, kreditkortsnummer o.s.v. komma i orätta händer.
- *Sprida virus eller andra oönskade program.* Den som har ett Wlan har troligen en brandvägg som skyddar mot attacker ifrån Internet men inte mot attacker som sker på insidan. Således kan virus och andra illvilliga program spridas i ett lokalt nätverk när nätägaren tror att denne är skyddad.
- *Komma åt intressanta filer.* Eftersom den som attackerar ett Wlan och lyckas ofta är på insidan av en eventuell brandvägg så kan denne komma åt intressanta dokument på filserverar o.s.v.
- *Nyfikenhet.* En del attacker har som enda mål att vara en intellektuell utmaning. Den som attackerar kanske inte utnyttjar sina färdigheter ytterligare.

---

<sup>13</sup>Personal Identification Nummer

## 4 Lösningar för att skydda sig

Som tidigare diskuterats så är hoten stora och riskerna många mot ett WLAN, se sid 6. Det vanligaste sättet att skydda sig är att använda WEP eller WPA men även att man kör hela WLAN:et som ett VPN. Ytterligare skydd är att låsa MACadresser och att använda ett hemligt SSID.

### 4.1 Wep

WEP använder antingen en 64- eller 128-bitars nyckel[5] för att kryptera trafiken. Krypteringen sker genom att använda RC4 vilket krypterar trafiken genom att göra en XOR på klartextdatat och nyckeln, resultatet blir en krypterad dataström. Den krypterade dataströmmen skickas över kommunikationskanalen, d.v.s. WLAN:et och mottagaren tar den krypterade dataströmmen och gör XOR med sin kopia av nyckeln och resultatet blir klartext[8]. Detta förfarande gör att den krypterade dataströmmen blir möjlig att attackera på flera sätt. Om en hacker byter ut en bit i den krypterade dataströmmen kommer motsvarende bit att bytas vid avkryptering. Dessutom kan den som avlyssnar trafiken göra XOR på två paket som sänts med samma nyckel och göra statistisk analys på resultatet för att få fram kryptonyckeln. Ju mer trafik som passerar desto bättre statistisk analys kan göras på trafiken. När någon bit av klartexten är avslöjad kan enkelt *all* annan krypterad trafik dekrypteras. I TCP/IP<sup>14</sup> paket kan stora delar av paketets innehåll gissas, då delar är samma eller nästan samma för alla paket som skickas. Detta underlättar avsevärt för att utföra en statistisk[9] analys av dataströmmen. WEP har skydd mot båda av dessa typer av attacker. För att kunna detektera förändring av datat så görs en integritetskontroll, IC<sup>15</sup>, av datapaketet. För att undvika krypering med samma kryptonyckel används en integritetsvektor, IV<sup>16</sup>, för att förstärka nyckeln och garantera att man inte krypterar med samma nyckel flera gånger. Tyvärr är implementeringen felaktig i WEP standarden vilket resulterar i en dålig säkerhet. Integritetskontrollen använder sig av CRC-32<sup>17</sup> vilket är en del av den krypterade trafiken. Problemet med CRC är att den är *linjär* vilket betyder att trots att man inte känner till klartexten kan man ändra i den krypterade dataströmmen så att CRC:n blir korrekt. Detta medför att mottagaren av datat inte kan detektera om datat ändrats under transporten. IVn är 24 bitar och en sådan liten nyckellängd medför att den kommer att återanvändas inom en ganska kort tidsrymd. Om man har en accesspunkt som har en hög trafiklast d.v.s. sänder 1500 bytes stora paket med 11 Mbit/s, kommer

---

<sup>14</sup>Transmission Control Protocol/Internet Protocol

<sup>15</sup>Integrity Check

<sup>16</sup>initialization vector

<sup>17</sup>Cyclic Redundancy Check

att upprepa IVn efter

$$\frac{1500 \cdot 8}{11 \cdot 10^6} \cdot 2^{24} \approx 18000 \text{sekunder} \approx 5 \text{timmar}.$$

Den datamängd som skickats under denna tidsrymd blir ca 24Gbyte vilket är en datamängd som en modern persondator hanterar med lätthet. I verkligheten kommer dock tiden och datamängden att vara kortare då paketlängden varierar. Eftersom WEP standarden inte säger något om hur många av dessa 24 bitar som verkligen skall användas har många tillverkare implementerat lösningar där inte alla bitar används[5], detta innebär att IVn kan komma att återkomma ännu oftare. En ytterligare begränsning är att många implementationer inte tillåter vilka värden som helst på IVn utan endast ASCII<sup>18</sup>, detta begränsar antalet IV ytterligare.

WEP standarden beskriver inte hur nyckelhanteringen skall skötas utan det enda kravet är att accesspunkten och noderna använder samma kryptoalgoritmer. Vanligen använder alla noder på nätverket samma nyckel. Idagsläget finns inga kommersiella produkter som byter nyckel[8] men man skulle kunna tänka sig att använda samma nyckelhantering som VPN d.v.s. ISAKMP<sup>19</sup>.

## 4.2 Starkare WEP

Ett försök att förbättra säkerheten i WEP är att öka antalet bitar, detta resulterar i att det dröjer längre innan IVn dyker upp igen. Ett antal företag har skapat proprietära lösningar såsom Agere Systems med 152-bitars WEP samt US Robotics och D-Link med 256-bitars WEP[13]. Eftersom dessa lösningar är proprietära kommer man att i behöva köpa all nätverksutrustning till sitt WLAN ifrån samma tillverkare. De fundamentala säkerhetsproblemen med WEP kvarstår dock, det tar bara längre tid att knäcka det.

## 4.3 WPA

På grund av de problem som WEP har har behovet av en ny lösning för att säkra WLAN både ifrån avlyssning och intrång varit stora. Ett antal lösningar har utvecklats men de har alla varit proprietära[10] vilket har medfört att utrustning ifrån olika tillverkare inte kunnat kommunicera. En sammanslutning av flera företag har tillsammans kommit överens om att använda en teknik som kalla WPA. Denna har ej ratificerats av något standardiseringsorgan men är ett snapshot av 802.11i som ännu inte är klar. WPA använder sig av TKIP<sup>20</sup> samt 802.11X. Denna kombination ger dynamisk nyckelkryptering och gemensam autentisering. Precis som WEP

<sup>18</sup>American Standard Code for Information Interchange

<sup>19</sup>Internet Security Association and Key Management Protocol

<sup>20</sup>Temporal Key Integrity Protocol

använder WPA RC4 för kryptering och CRC för kontroll av paketen. TKIP medför följande:

- *48 bitars initieringsvektor* Precis som WEP har WPA en initieringsvektor men den är 48 bitar istället för 24 vilket minskar sannolikheten att två stycken likadana IVs dyker upp som en hacker kan utnyttja för att göra statistiska beräkningar på.
- *Nyckelskapande och distribution sker per paket* WPA genererar en unik nyckel för varje 802.11 paket. Detta för att undvika att samma nyckel används under längre tid som i WEP.
- *Meddelande integritet* WPA har en förbättrad rutin för att säkerställa att ett paket inte har förändrats. Detta sker genom att lägga till en MIC<sup>21</sup> i paketet som inte är lika lätt att förändra utan detektering, som i WEP.

Ett problem som WPA inte löst är DoS<sup>22</sup>-attacker. Om en hacker sänder två paket inom en sekund som innehåller en felaktig krypteringsnyckel kommer alla uppkopplingar att tas ned av accesspunkten under en minut. När väl 802.11i standarden är färdigutvecklad kommer den att vara bakåtkompatibel med WPA. 802.11i kommer även att innehålla stöd för AES<sup>23</sup> vilket kommer att kräva en stödprocessor. WPA har samma sårbarhet mot attacker som alla system som använder lösenord[12]. Då vi människor som skall hitta på ett lösenord gärna använder ett ord som kan gissas så ger detta en möjlighet för en hacker att gissa lösenordet genom att utnyttja kunskaper om den som har hittat på lösenordet eller att använda ordlistor<sup>24</sup>. För att skydda sig mot denna typ av attack måste lösenordet vara skyddat och extremt svårt att gissa, d.v.s. lösenordet skall inte sitta på en postitlapp under tangetbordet eller vara ett ord som förekommer i ett lexikon.

#### 4.4 VPN

En lösning för att komma runt problematiken med WEP kryptering skulle kunna vara att använda VPN<sup>25</sup> mellan noderna och accesspunkten eller mellan noderna och en central VPN-server se fig3. Efter en snabb undersökning på webshopar där nätverksutrusning säljs<sup>26</sup> hittades *inga* WLAN-accesspunkter som klarade att köra VPN till sin noder. Således är den praktiska lösningen en central VPN-server. VPNs säkerhet beror på vilken krypteringsteknologi som används. Använder man t.e.x. 3DES eller AES som kryptering så är den enda kända metoden att knäcka dessa brute-force,

---

<sup>21</sup>Message Integrity Code

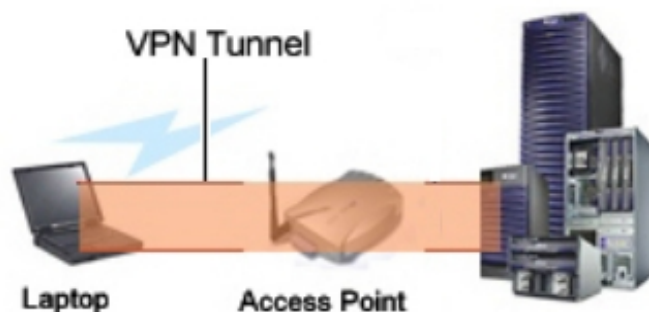
<sup>22</sup>Denial of Service

<sup>23</sup>Advanced Encryption Standard

<sup>24</sup>Dictionary Attacks

<sup>25</sup>Virtual Private Network

<sup>26</sup><http://www.dustin.se> <http://www.inwarehouse.se/>



Figur 3: VPN tunnel i WLAN

d.v.s. att testa med ett antal nycklar tills man får fram klartexten[9]. Då man kan vid konfigureringen av VPN:et kan sätta en lång nyckellängd behövs mycket stora resurser för att kunna knäcka dessa krypton. Det stora problemet med VPN är den relativt krångliga konfigureringen. För många är det en oöverstiglig tröskel och i praktiken är det bara företag med kunning personal och tillräckliga resurser som har möjlighet att utnyttja VPN baserad WLAN. En annan nackdel är att den komplicerade krypteringen/dekrypteringen kräver så stora resurser av noderna att detta kan bli en flaskhals i kommunikationen se tabell2.

<i>Kryptering</i>	<i>Nyckellängd</i>	<i>Hastighet (Mbps)</i>
DES	56	9
3DES	168	3
RC4	Varierar	45

Tabell 2: Hastighetsjämförelse av symmetrisk krypering på en Pentium II

#### 4.5 Låsta MAC-adresser

Varje nätverskort har ett unikt id, kallat MAC<sup>27</sup>-address. Denna är programmerad i hårdvaran på kortet och kan endast med relativ svårighet ändras genom omprogramering av den krets som innehåller MAC-adressen. MAC-adressen används för kommunikation mellan noderna på ett LAN så att datat skickas till rätt nod. I de flesta accesspunkter kan man låsa så att endast godkända MAC-adresser får ansluta till accesspunkten. Genom denna åtgärd får man inget skydd mot avlyssning men ett visst skydd mot intrång. Då de flesta nätverkskort kan byta MAC-address i mjukvaran och

<sup>27</sup>Medium Access Control

då hårdvaruadressen inte används överhuvudtaget får detta skydd anses som mycket rudimentärt[11].

## 4.6 SSID

För att kunna använda ett WLAN behöver man känna till nätets SSID. De flesta WLAN accesspunkter har en standardinställd SSID som tillverkaren av WLAN utrustningen konfigurerar vid tillverkningen, se tabell 3. Skulle administratören av nätet ha ändrat på SSID finns det ett antal verktyg för att ta reda på SSID. Detta medför att SSID:et får anses som ett svagt skydd mot obehörigt användande av ett WLAN.

<i>Tillverkare</i>	<i>Förinställt SSID</i>
Cisco	tsunami
3Com	101
Lucent/Cabletron	RoamAbout
Compaq	Compaq
Addtron	WLAN
Intel	intel
Linksys	linksys

Tabell 3: Förinställd SSID

## 5 Attackmetoder

Att hitta WLAN att attackera är enkelt, det räcker med att ta en laptop med ett WLAN nätverkskort och passera byggnader och platser där man misstänker att det kan finnas WLAN. I laptopen har man installerat ett enkelt program som mäter fältstyrkan och när man väl hittat ett nät utnyttjar man de eventuella svagheter för att utföra sin attack. Man talar om[7]: War-driving, war-walking och war-flying beroende på vilket färdssätt som används för att leta upp sårbara WLAN. När ett WLAN har hittats kan man markera det s.k. war-chalking<sup>28</sup>, så att andra hackers kan använda samma WLAN.

### 5.1 Attack av WEP

Det finns ett antal verktyg för att analysera WLAN trafik och knäcka WEP, en snabb sökning på Google gav följande exempel:

- aircrack WEP knäckning. <http://www.cr0.net:8040/code/network/>

<sup>28</sup>För symboler m.m. se <http://www.blackbeltjones.com/warchalking/index2.html>

- airsnort WLAN Sniffer<sup>29</sup>, WEP knäckning. <http://airsnort.shmoo.com/>
- netstumbler, ett verktyg för att känna av Wlan nätverk i omgivningen. <http://www.netstumbler.com/downloads/>
- wepcrack, WEP knäckning. <http://sourceforge.net/projects/wepcrack/>

## 6 Empiriskt test

Författaren av denna uppsats ville testa hur många Wlan som kunde hittas ifrån köket i ett villområde i Huddinge och om eventuella skydd skulle kunna knäckas. Ett Wlan PCMCIA kort, 3Com, lånades av vänner. Netstumbler installerades och tre nät hittades, varav två var skyddade med 128-bitars Wep och ett var totalt oskyddat. Efter att ha testat att ansluta till det oskyddade nätet kunde ftp.sunet.se pingas och surfning fungerade utmärkt, då detta gränsar till dataintrång kopplades nätet ifrån. För att försöka knäcka WEP krypteringen i de två andra näten installerades Airsnort för windows, tyvärr så stödjer inte Airsnort för windows 3Com kort och tiden räckte inte till för att installera Linux på den bärbara datorn som fanns tillgänglig.

## 7 Slutsatser

Säkerheten i WLAN är lätt att knäcka. Om man vill använda sig av ett WLAN är det oerhört viktigt att man gör en hot- och riskbildsanalys för att försöka ta reda på om fördelarna överväger nackdelarna. Den säkerhet som alla tillverkare stödjer är 40- respektive 128-bitars Wep och dess säkerhet är minimal om den som attackerar bara får lite tid på sig. Visserligen finns det starkare skydd som 256-bitars Wep, WPA och VPN men dessa medför ofta speciallösningar som inte är bakåtkompatibel med äldre utrustning, är proprietär så endast en viss tillverkares utrustning fungerar ihop eller är så komplicerad att det krävs en IT-avdelning hos ett företag för att få det att fungera. Ett stort problem under faktasökande till uppsatsen är att det dykt upp motsägelser eller att informationen som hittats blivit omodernt. Inom WLAN området är utvecklingen mycket snabb och många företag vill inte vänta på att standardiseringsorganisationer skall ta beslut på vilken lösning som skall gälla, detta medför att floran av inkompatibel utrustning ökar ju mer tiden går. En tendens verkar vara att de som konfigurerar WLAN accesspunkter väljer "minsta gemensamma nämnare" Risken finns att delar av denna uppsats kommer att vara omodern inom en snar framtid.

---

<sup>29</sup>En sniffer är ett verktyg som används för att avlyssna trafik

## A Referenser

### Referenser

- [1] Stuart McClure, Joel Scambray och George Kurtz. *Hacking exposed, Network Security Secrets & Solutions. Fourth Edition*. Mc Graw Hill Osbourne.
- [2] Wireless Networking Overview  
<http://support.intel.com/support/wireless/wlan/sb/cs-008165.htm>
- [3] WLAN Technical basics  
[http://www.wimo.com/cgi-bin/verteiler.pl?url=wlanbasics\\_e.htm](http://www.wimo.com/cgi-bin/verteiler.pl?url=wlanbasics_e.htm)
- [4] Wireless LAN Standards  
[http://www.webopedia.com/quick\\_ref/WLANStandards.asp](http://www.webopedia.com/quick_ref/WLANStandards.asp)
- [5] WLAN Security: Wide Open  
<http://www.tomsnetworking.com/network/20020719/>
- [6] RC4 From Wikipedia, the free encyclopedia.  
<http://en.wikipedia.org/wiki/RC4>
- [7] Wireless LAN Security FAQ  
[http://www.iss.net/wireless/WLAN\\_FAQ.php](http://www.iss.net/wireless/WLAN_FAQ.php)
- [8] Security of the WEP algorithm  
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- [9] William Stallings. *Cryptography and Network Security, Principles and practices. Third edition* Prentice Hall, 2003.
- [10] WPA Security Enhancements  
<http://www.wi-fiplanet.com/tutorials/article.php/2148721>
- [11] Is Your Wireless Network Secure?  
<http://www.sans.org/rr/papers/68/149.pdf>
- [12] Dictionary Attacks Against WPA / 802.11i  
<http://peertech.org/node/view/48>
- [13] Beyond WEP  
<http://www.wi-fiplanet.com/tutorials/article.php/1490451>

## B Förkortningar, Ordlista

**802.11** Standard för Wlan. Definierat och beskrivet av IETF.

**AES** Advanced Encryption Standard, är en symmetrisk krypteringsalgoritm som är utvald som standardalgoritm att ersätta DES.

**ASCII** American Standard Code for Information Interchange.

**Brute-force** En attackmetod där man testar med olika nycklar utan att nycklarna tillhör någon speciella mängd.

**Dictionary Attacks** En attackmetod där man tar en ordlista och testar ord för ord om lösenordet är något av dessa, jmf Brute-force.

**DoS** Denial of Service, avser en attack med en dator, ett nätverk el dyl med syfte att slå ut offret, oftast genom överbelastning.

**Hub** Nav, en enhet på nätverk som kopplar ihop flera noder med varandra. En hub är "korkad" och kan inte skilja ut vilken trafik som skall vart utan skickar all trafik den får in, ut på alla anslutna linjer.

**IETF**, Internet Engineering Task Force. Ett standardiseringsorgan för internetteknologier.

**IV**, initialization vector.

**ISAKMP** Internet Security Association and Key Management Protocol

**MAC** Medium Access Control

**MAC-adress** En adress som används på länknivån i OSI modellen för att adressera enheter i ett nätverk. Varje nätverksenhet som tillverkas har en unik MAC-adress, den kan oftast ändras m.h.a. mjukvara eller ett systemkommando.

**MIC** Message Integrity Code, används för att skydda integriteten i ett WPA-krypterat meddelande.

**Nod** En nätverksansluten enhet, kan t.ex. vara en dator, en skrivare, en telefon, en WLAN accesspunkt.

**RC4** En kryptoalgoritm som använder XOR på klartexten och nyckeln[6].

**Router** Enhet som väljer väg för och vidarebefordrar data i ett datornät, kan vara en dator med flera nätverksort

**Sniffer** En sniffer är ett verktyg som används för att avlyssna trafik.

**SOHO** Small Office Home Office, en beteckning på små kontor och hemmakontor.

**SSID** Service Set Identifier, namn på ett Wlan. Kan vara upp till 32 tecken långt och bestå av bokstäver och siffror.

**TKIP** Temporal Key Integrity Protocol, arbetar på MAC-lagret med administrationen av krypteringsnycklar, så att varje användare får en egen krypteringsnyckel som dessutom byts ut efter en viss tid.

**VPN** Virtual Private Network. Virtuellt nätverk, man kan koppla ihop flera nätverk med varandra via t.ex. internet så att de verkar vara samma nätverk för användare och datorer.

**WEP** Wired equivalent privacy. Standard för att kryptera trafik mellan noder i ett Wlan. Kan använda 64- eller 128-bitars nycklar.

**WLAN** Wireless Local Area Network