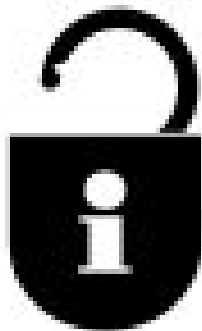


ÖREBRO UNIVERSITET

Institutionen för Ekonomi,
Statistik och Informatik (ESI)
C-uppsats, Informatik C, HT01
Handledare: Ella Kolkowska
2002-01-18

Säkerhet i integrerade trådlösa nätverk

- är VPN en lösning?



Författare:
Lydia Eliasson 761128
Anna Stenquist 760505

SAMMANFATTNING

De trådlösa teknikerna Bluetooth och WLAN, vilka är baserade på radioteknik, var årets huvudattraktion på Comdex-mässan. Inget pekar på att detta bara är en fluga och att vi kommer att överge dessa tekniker för att återigen endast använda traditionella kabelnätverk. Idag kan dock det ultimata trådlösa nätverket aldrig uppnås med en teknik, utan olika nätverksteknologier kompletterar varandra. Det är möjligt att integrera olika lösningar såsom Bluetooth och WLAN för att uppnå maximal funktionalitet. Detta kan göras via så kallade access points. Access points som fungerar för både Bluetooth och WLAN finns ännu inte på marknaden men företaget Possio beräknas lansera en sådan under år 2002.

I och med att dessa båda tekniker integreras skapas en efterfrågan på en säkerhetslösning som fungerar i båda nätverksteknikerna. Vi har i denna uppsats valt att undersöka om VPN kan täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk, det vill säga nätverk där Bluetooth- och WLAN-nät integreras via access points. Vidare har vi undersökt hur olika VPN-lösningar passar i de vanligaste användningssituationerna för integrerade trådlösa nätverk.

För att kunna avgöra om VPN täcker de säkerhetsluckor som finns i integrerade trådlösa nätverk har vi först beskrivit teknikerna Bluetooth och WLAN samt säkerhetsaspekterna i de separata nätverksteknikerna. Genom att jämföra och diskutera dessa säkerhetsaspekter har vi kommit fram till två säkerhetskriterier som måste uppfyllas för att göra ett integrerat trådlöst nätverk säkert. Dessa två kriterier är:

1. En obehörig ska inte kunna ta sig in i det trådlösa nätverket och avlyssna informationen.
2. Om obehörig ändå gör ett intrång i det trådlösa nätverket ska denne inte förstå vad som sägs.

Efter att undersökt VPN och dess olika funktioner kom vi fram till att VPN uppfyller dessa två kriterier och således täcker de säkerhetsluckor som existerar i integrerade trådlösa nätverk.

För att undersöka hur väl olika VPN-lösningar passar i de vanligaste användningssituationerna genomförde vi en mindre enkätundersökning. Detta för att få en bild av vilka användningssituationer som kommer att dominera i framtidens integrerade trådlösa nätverk.

De vanligaste situationerna var privat användning i hemmet, privat användning på det egna företaget samt användning i tjänsten på det egna företaget. Det finns VPN-lösningar som passar i dessa olika användningssituationer och det finns således inget hinder för att implementera VPN i integrerade trådlösa nätverk.

ORDLISTA

3des – symmetrisk krypteringsalgoritm som används i *IPSec*.¹

Access point (AP) – En *station* som transporterar data mellan ett trådlöst nätverk och ett fysiskt nätverk, eller mellan två trådlösa nätverk.²

ACL – Access Control List. Lista med *MAC-adresser* på de *stationer* som är behöriga att använda nätverket.³

Ad hoc – ”för detta särskilda (och tillfälliga) ändamål”.⁴

Bluetooth – en trådlös radioteknik som stödjer både data- och röstöverföring.⁵

CPU – Central Processing Unit.⁶ En dators processor.

DSSS – Den sändningsteknik som används i de flesta *WLAN*.⁷

FHSS – En sändningsteknik som används av *Bluetooth* och i vissa fall av *WLAN*.⁸

Gateway – fungerar som en tolk mellan olika typer av protokoll.⁹

Hotspot – ett område där det går att koppla upp sig mot ett nätverk med hjälp av någon trådlös nätverksteknik.¹⁰

IPSec – inkapslingsprotokoll för *VPN*.¹¹

IrDA – infrarött ljus.

ISM-bandet – det licensfria frekvensband som *WLAN* och *Bluetooth* sänder över.¹²

LAN – Local Area Network. Ett lokalt nätverk av datorer och kringutrustning som skrivare med mera.¹³

MAC – Medium Access control. En del av länkskiktet i OSI-modellen.¹⁴

MAC-adress – 48 bits adress som identifierar ett *NIC*.¹⁵

Mbs – Måtenhet för dataöverföringshastighet, betyder Mega bits per second. Förkortas även Mbps eller Mb/s.

Microcell – Det område som täcks av en sändare i ett trådlöst lokalt nätverk.¹⁶

NIC – Network Interface Card, det vill säga ett nätverkskort.¹⁷

Piconet – nätverkstopologi i *Bluetooth*, med minst två och max åtta enheter sammankopplade.¹⁸

PKI – Public Key Infrastructure.¹⁹

Roaming – Förflyttning av en trådlös enhet mellan olika *microcells*.²⁰

¹ OpenBSD

² WLANA

³ Wavelink, Wireless Network Security

⁴ Nationalencyklopedien

⁵ Miller, M., Discovering Bluetooth

⁶ Englander, I., The Architecture of Computer Hardware and Systems Software

⁷ PCTechGuide, Wireless Networks

⁸ Miller, M., Discovering Bluetooth

⁹ Mårild, K., Possio

¹⁰ Mårild K., Possio

¹¹ Tyson, J., How Virtual Private Networks Works

¹² Miller, M., Discovering Bluetooth

¹³ Englander, I., The Architecture of Computer Hardware and Systems Software

¹⁴ Ottosson, B., Internet & TCP/IP

¹⁵ Jensen, S. m fl, Datakommunikation

¹⁶ WLANA

¹⁷ Jensen, S. m fl, Datakommunikation

¹⁸ Miller, M., Discovering Bluetooth

¹⁹ Lindqvist, J., Nätverk och Kommunikation, nr 18, 2001

SAFER+ - Secure And Fast Encryption Routine. En symmetrisk krypteringsalgoritm, för *Bluetooth*.²¹

Scatternet – nätverkstopologi i *Bluetooth* där flera *Piconet* är sammankopplade.²²

Spread Spectrum – tekniker för att dela upp data som ska sändas över hela det tillgängliga frekvensbandet.²³

Station (STA) – Enhet med nätverkskort avsett för *WLAN*.²⁴

Topologier – hur noder i ett nätverk är sammankopplade och grupperade.²⁵

VPN - står för *Virtuellt Privat Nätverk* och är ett sätt tunnla information för att på ett säkert sätt överföra den över ett osäkert medium.²⁶

WEP - Wired Equivalent Privacy. WEP är en symmetrisk krypteringsalgoritm där samma algoritm och nyckel används för både kryptering och dekryptering av data.²⁷

WLAN - fungerar som ett *LAN* med undantaget att enheterna i nätverket kommunicerar via elektromagnetiska vågor istället för via kablage.²⁸

WISP – Wireless Internet Service Provider. Ett företag som tillhandahåller trådlös access till Internet. Telia är ett exempel på en WISP.²⁹

²⁰ WLANA

²¹ Kumria, A., University of Technology, Sydney

²² Miller, M., Discovering Bluetooth

²³ Ewert, M., Datakommunikation

²⁴ The linux-wlan Company

²⁵ Englander, I., The Architecture of Computer Hardware and Systems Software

²⁶ Tyson, J., How Virtual Private Networks Works

²⁷ Cisco Systems

²⁸ Cisco Systems

²⁹ Mårild, K., Possio

INNEHÅLLSFÖRTECKNING

1	INLEDNING	6
1.1	PROBLEMBAKGRUND.....	6
1.2	PROBLEMDISKUSSION.....	7
1.3	FRÅGESTÄLLNING	7
1.4	ANALYS AV FRÅGESTÄLLNING	7
1.5	AVGRÄNSNING	8
1.6	SYFTE.....	9
1.7	INTRESSEENTER/MÅLGRUPP	9
1.8	KUNSKAPSBIDRAG	9
2	PERSPEKTIV	10
2.1.1	<i>Ordval</i>	11
2.1.2	<i>Koppling till befintlig kunskap</i>	11
2.1.3	<i>Centrala begrepp</i>	11
2.2	ALTERNATIVA PERSPEKTIV	12
3	METOD	14
3.1	TILLVÄGAGÅNGSSÄTT.....	15
3.1.1	<i>Integrerade trådlösa nätverk</i>	16
3.1.2	<i>Virtuella Privata Nätverk</i>	17
3.1.3	<i>Användningssituationer</i>	18
3.1.4	<i>Analys</i>	20
3.2	KÄLLKRITIK	21
3.3	VALIDITET.....	21
3.4	RELIABILITET	22
4	INTEGRERADE TRÅDLÖSA NÄTVERK	23
4.1	OSI-MODELLEN.....	23
4.2	BESKRIVNING AV WLAN- OCH BLUETOOTH-TEKNIKERNAS.....	24
4.3	INTEGRERING AV BLUETOOTH OCH WLAN	25
4.4	SÄKERHET	28
4.4.1	<i>Vilka säkerhetsrisker föreligger för WLAN och Bluetooth?</i>	28
4.4.2	<i>Lösningar</i>	29
5	VIRTUELLA PRIVATA NÄTVERK	32
5.1	INLEDNING	32
5.2	TYPEN AV VPN	33
5.3	VPN-SÄKERHET	33
5.3.1	<i>Brandväggar</i>	33
5.3.2	<i>Autenticering</i>	34
5.3.2.1	Autenticeringsmetoder	34
5.3.3	<i>Tunnling</i>	35
5.3.3.1	IPSec.....	35
5.3.3.2	Exempel på upprättande av tunnel mellan server och klient.....	36
5.3.4	<i>Kryptering</i>	36
5.4	VPN I TRÅDLÖSA NÄTVERK	38

5.5	SPECIELLA EGENSKAPER HOS EN VPN-LÖSNING ANPASSAD SÄRSKILT FÖR TRÅDLÖSA NÄTVERK.....	39
6	ANVÄNDNINGSSITUATIONER.....	40
6.1	VILKA ANVÄNDNINGSSITUATIONER ÄR VANLIGAST?	40
7	ANALYS	43
7.1	KAN VPN TÄCKA DE SÄKERHETSLUCKOR SOM FINNS I INTEGRERADE TRÅDLÖSA NÄTVERK?	43
7.1.1	<i>Integrerade trådlösa nätverk.....</i>	<i>43</i>
7.1.2	<i>Säkerhetsaspekter.....</i>	<i>44</i>
7.1.2.1	Kriterium 1 – neka obehörig åtkomst till nätverket	45
7.1.2.2	Kriterium 2 – göra data oläslig för obehörig.....	45
7.1.2.3	Tunnling – Kriterium 1 och 2.....	45
7.2	HUR PASSAR OLIKA VPN-LÖSNINGAR I DE VANLIGASTE ANVÄNDNINGSSITUATIONERNA FÖR INTEGRERADE TRÅDLÖSA NÄTVERK?	46
7.2.1	<i>Användningssituationer för privat användare</i>	<i>46</i>
7.2.2	<i>Användningssituationer för tjänsteanvändare</i>	<i>47</i>
7.2.3	<i>Icke-mobil/Stationär användning.....</i>	<i>48</i>
7.2.4	<i>Mobil användning</i>	<i>49</i>
8	SLUTSATSER.....	50
9	DISKUSSION	52

KÄLLFÖRTECKNING

1 INLEDNING

1.1 Problembakgrund

De trådlösa teknikerna WLAN och Bluetooth, vilka är baserade på radioteknik, var årets huvudattraktion på Comdex-mässan³⁰. Inget pekar på att detta bara är en fluga och att vi kommer att överge dessa tekniker för att återigen endast använda traditionella kabelnätverk.

Trådlösa nätverk kan användas på flera olika sätt. Det kan vara en ersättning för kablar på ett företag så att användaren kan vara mer flexibel, till exempel går det lättare att byta plats på kontoret eller att ta med datorn på mötet och fortfarande ha tillgång till nätverket. Vidare underlättar det även för användaren på fältet, både privatpersoner och människor i tjänsten. Dessa kan röra sig fritt och ändå ha tillgång till nätverksuppkoppling. Ett exempel på detta skulle kunna vara att med sin handdator skicka ett dokument till en skrivare på den plats användaren råkar befinna sig utan att behöva koppla ihop enheterna fysiskt.

Idag kan dock det ultimata trådlösa nätverket aldrig uppnås med en teknik, utan olika nätverksteknologier kompletterar varandra. Det är möjligt att integrera olika lösningar, till exempel WLAN och Bluetooth, för att få tillgång till alla önskade funktioner. Detta kan göras via så kallade access points. Access points som fungerar för både Bluetooth och WLAN finns ännu inte på marknaden, men beräknas komma under år 2002³¹.

De nya teknologierna introducerar nya möjligheter och med dem nya säkerhetsrisker. Kabeln har hittills stått som en slags garant för säkerhet. För att avlyssna trafiken i ett fysiskt nätverk måste inkräktaren vara mycket nära kabeln och för att störa datatrafiken krävs fysiska åtgärder, såsom att klippa av kabeln. I trådlösa nätverk finns inga kablar och en inkräktare är därför inte lika lätt att upptäcka och således blir det mer komplicerat att skydda nätverket. Det går dock att skydda sig mot säkerhetsriskerna som uppstår vid trådlös kommunikation.

Vissa säkerhetsrisker kan lösas om standarden för Bluetooth respektive WLAN följs. Ett nytt problem uppstår dock om näten ska integreras via access points. Standarden föreskriver endast hur säkerhet kan uppnås inom ett nätverk där endast Bluetooth-enheter kommunicerar med varandra.

Även standarden för WLAN behandlar endast den egna tekniken och reglerar därför bara trafiken mellan WLAN-enheter. Den svaga punkten är framförallt access points eftersom det är de som förmedlar data samt ger tillträde till nätverket. Är en access point dessutom inte bara en länk i ett WLAN-nät utan även en länk till ett fysiskt nätverk eller ett Bluetooth-nät så är det extra farligt att den utgör en säkerhetslucka. Detta eftersom enheter med värdefullt innehåll, såsom databaser eller applikationsservrar ofta ingår i det fysiska nätverket.

De två teknikerna skiljer sig åt på flera punkter, men ett har de gemensamt – luften, i vilken radiovågorna färdas. Luften är liksom Internet ett osäkert medium. På Internet används VPN-tekniken för att skydda informationen. VPN står för Virtuellt Privat Nätverk och syftet är att

³⁰ Ricknäs, M., Computer Sweden, nr 118, 2001-11-12

³¹ Mårild, K., Possio

simulera egenskaperna hos ett privat nätverk över ett osäkert medium. Skulle inte VPN då kunna vara ett alternativ för ökad säkerhet vid kommunikation mellan trådlösa nätverk?

1.2 Problemdiskussion

Vi vill studera teknikerna Bluetooth och WLAN samt säkerhetsrisker förknippade med dessa. Detta gör vi för att få en bild av vilka säkerhetsrisker som kan existera i integrerade trådlösa nätverk. Genom att studera säkerhetsrisker i Bluetooth respektive WLAN kan vi se likheter och skillnader mellan de båda teknologierna. Utifrån detta kan vi göra oss en bild av vilka risker som kommer att existera i ett nätverk där båda dessa tekniker ingår. Både Bluetooth och WLAN innehåller åtgärder mot de risker som är förknippade med respektive teknologi. Dessa åtgärder fungerar dock endast på den teknik de är utvecklade för. Vi vill därför undersöka om VPN kan vara en säkerhetslösning för integrerade trådlösa nätverk. Eftersom VPN inte är beroende av nätverkstyp skulle det kunna vara en lösning som åtgärdar funna säkerhetsbrister för båda nätverkstyperna när de integrerats i ett nätverk.

Vi vill undersöka hur VPN passar i de vanligaste användningssituationerna för integrerade trådlösa nätverk. Även om det visar sig att VPN är en tänkbar lösning på säkerhetsrisker i integrerade trådlösa nätverk så behöver inte det innebära att VPN passar i dessa nätverk rent tekniskt och praktiskt. Med andra ord skulle VPN kunna fungera rent tekniskt men i praktiken vara komplicerat att använda i till exempel en handdator.

I integrerade trådlösa nätverk med WLAN och Bluetooth är användarna mobila vilket gör att användningssituationerna kan skilja sig från de där VPN traditionellt har använts. Samma lösning som är praktisk på en persondator som ständigt står på ett kontor behöver inte vara lika praktisk för en handdator på ett café.

1.3 Frågeställning

Våra huvudfrågor i denna uppsats är:

- Kan VPN täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk?
- Hur passar olika VPN-lösningar i de vanligaste användningssituationerna för integrerade trådlösa nätverk?

1.4 Analys av frågeställning

Vår första huvudfråga är:

- *Kan VPN täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk?*

För att ta reda på om VPN kan täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk måste vi först beskriva vad ett integrerat trådlöst nätverk är. I denna frågeställning menar vi att ett integrerat trådlöst nätverk endast består av Bluetooth- och WLAN-enheter samt en access point som fungerar som en gateway mellan dessa tekniker. En gateway fungerar som en tolk mellan olika nätverkstyper. En access point är en enhet som kan sända och ta emot data och används för att koppla ihop olika trådlösa nätverk eller ett trådlöst och ett fysiskt nätverk. Det skulle även kunna ingå infraröd eller någon annan trådlös teknik i ett integrerat trådlöst nätverk. När vi beskriver ett integrerat trådlöst nätverk gör vi detta genom att beskriva de komponenter som ett sådant nätverk består av, nämligen Bluetooth, WLAN och access points.

Efter att ha beskrivit integrerade trådlösa nätverk måste vi ta reda på vilka säkerhetsluckor som finns i Bluetooth- respektive WLAN-nät. En säkerhetslucka är detsamma som en säkerhetsrisk eller ett säkerhetsproblem. Dessa begrepp innebär en svaghet som kan utnyttjas av en inkräktare för att avlyssna eller göra intrång i nätverket. Anledningen till att vi undersöker säkerhetsluckor i teknikerna var för sig är att det i dagsläget inte existerar några nätverk där dessa två tekniker är integrerade. När säkerhetsluckorna hos respektive teknik är kartlagda kan vi få en uppfattning om vilka säkerhetsluckor som kommer att finnas i integrerade trådlösa nätverk. Utifrån dessa säkerhetsluckor kan vi sedan formulera säkerhetskriterier. Säkerhetskriterier är sådana kriterier som måste uppfyllas för att ett nätverk ska anses vara säkert. Vi måste därefter ta reda på och beskriva tekniken VPN är för att kunna avgöra om VPN täcker de säkerhetskriterier vi har ställt upp.

Vår andra huvudfråga är:

- *Hur passar olika VPN-lösningar i de vanligaste användningssituationerna för integrerade trådlösa nätverk?*

Denna huvudfråga blir endast intressant om VPN kan täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk, se huvudfråga 1.

För att ta reda på hur olika VPN-lösningar passar i de vanligaste användningssituationerna för integrerade trådlösa nätverk måste vi först skapa oss en bild av vilka användningssituationer som kommer att dominera för integrerade trådlösa nätverk. Detta gör vi genom undersöka vilka användningssituationer som är vanligast i Bluetooth- respektive WLAN-nät i dagsläget. Användningssituationerna som är vanligast i dessa nät torde även komma att bli vanligast i integrerade trådlösa nätverk. Med användningssituation menar vi den plats där tekniken används samt i vilket syfte denna används. När vi sedan undersöker om VPN passar i dessa användningssituationer så fokuserar vi på hur de passar rent tekniskt och praktiskt. Tekniska aspekter kan vara sådana som vilka protokoll som används. Praktiska aspekter kan exempelvis utgöras av utrymmes- eller kapacitetskrav.

1.5 Avgränsning

Vi har valt att endast behandla teknikerna Bluetooth och WLAN. Det finns andra trådlösa tekniker för dataöverföring, främst via GSM-nätet, och en heltäckande VPN-lösning kan eventuellt vara applicerbart även för dessa typer av nät. Detta har vi dock valt att inte undersöka då vårt största intresse är att finna lösningar för nätverk med inslag av just Bluetooth och WLAN. Detta i sin tur beror på att vi samarbetar med företaget Possio som har utvecklat en access point för just dessa två tekniker. I de integrerade trådlösa nätverk som vi har valt att titta på kan även infrarött ljus användas för nätverksuppkoppling. Detta har vi dock avgränsat oss från, eftersom vi har fått uppfattningen att detta inte är så vanligt.

Beskrivningen av WLAN och Bluetooth är endast till för att läsaren ska kunna förstå säkerhetsaspekterna med dessa tekniker. Tre viktiga aspekter för nätverks säkerhet är avlyssning, intrång och störning. De säkerhetsaspekter vi tar upp handlar om avlyssning och intrång. Vi har avgränsat oss från säkerhetsrisker såsom störning av trafiken med hjälp av starka sändare som hindrar radiovågorna och koncentrerat oss på intrång och avlyssning. Störning är i sig ett stort område och det skiljer sig från avlyssning och intrång på flera viktiga punkter. Störning ligger närmare området för radioteknik, medan avlyssning och intrång

ligger inom det klassiska området nätverkssäkerhet. Störning ger inte tillgång till konfidentiell information, men är ändå en säkerhetsrisk.

Även beskrivningen av VPN är avgränsad till aspekter som rör avlyssning och intrång, till exempel autentisering och kryptering. Vi är inte intresserade av hur säkra säkerhetsfunktionerna i VPN är, till exempel hur lätt det kan vara att knäcka en krypteringsalgoritm. Vi är endast intresserade av om VPN innehåller funktioner som löser de säkerhetsbrister vi tittar på i integrerade trådlösa nätverk.

Vi vill inte heller utröna om VPN är bättre eller sämre än andra tänkbara säkerhetslösningar för integrerade trådlösa nät utan endast undersöka om det kan vara ett lämpligt alternativ. Vi bygger dock vårt resonemang på att VPN eventuellt kan lösa säkerhetsriskerna i hela det integrerade trådlösa nätet. Detta skulle vara en fördel gentemot de säkerhetslösningar som är nätverksspecifika och alltså inte kan täcka ett helt integrerat nätverk.

1.6 Syfte

Syftet med denna uppsats är att undersöka om VPN kan täcka de säkerhetsluckor som finns i Bluetooth och WLAN när dessa två typer av trådlösa nätverk integreras via access points. Vidare skall vi undersöka hur olika VPN-lösningar passar i de vanligaste användningssituationerna för integrerade trådlösa nätverk.

1.7 Intressenter/Målgrupp

Uppsatsen är skriven i samarbete med företaget Possio som bland annat utvecklar access points för Bluetooth och WLAN. I uppsatsen behandlas säkerhetsrisker och tänkbara lösningar för nätverk som implementerar Bluetooth- och/eller WLAN-teknologi och Possio ligger därför självklart i uppsatsens målgrupp.

Resultatet av detta arbete kan även vara intressant och användbart för andra informatikstudenter, nu och kommande terminer, som har intresse av säkerhet i trådlösa nätverk. Andra företag i branschen är också tänkbara intressenter.

1.8 Kunskapsbidrag

Denna uppsats ska ge en beskrivning av integration av Bluetooth- och WLAN- nät. Därefter ska vi undersöka om VPN kan lösa säkerhetsproblemen i sådana integrerade nätverk.

Vi skall i uppsatsen redogöra för de användningssituationer som är vanligast i Bluetooth- och WLAN-nät. Detta för att sedan avgöra om någon VPN-lösning skulle vara lämplig i dessa situationer.

2 PERSPEKTIV

Vårt perspektiv påverkas av allt från uppväxt till tidigare kurser vid universitetet. Det kan vara svårt att klart och tydligt skriva ner vilket perspektiv man har eftersom det till viss del är omedvetet. Vi har dock försökt att så tydligt som möjligt klargöra de delar av vårt perspektiv som i störst utsträckning kan påverka utformningen av och upplägget på denna uppsats.

Vi är båda teknikintresserade och har en positiv grundinställning till teknisk utveckling. Exempelvis menar vi att utveckling av ny IT-teknologi är något positivt även om denna till en början kan ha stora brister. Vi ser ett problem eller en brist hos ett system som en möjlighet till fortsatt utveckling istället för ett hinder.

Under cirka fyra år har vi studerat vid universitet och under de senaste två åren har vi inriktat oss mot informatik. Vi har något olika inriktning på vår studiegång, vilket gör att vi tillsammans har ett brett kunskapspektrum med allt från maskinteknik till pedagogik.

Vårt perspektiv påverkas även av företaget Possios intressen. Possio är ett företag som utvecklar och tillverkar lösningar för trådlösa nätverk. De har utvecklat den första access pointen som även fungerar som en Gateway mellan Bluetooth och WLAN och på så vis gör det möjligt att integrera dessa två nätverkstyper. Det är i samarbete med dem vi undersöker säkerheten i denna typ av trådlösa nätverk. Vi hade eventuellt inte valt att behandla VPN om inte detta förslag hade kommit från en av teknikexperterna på företaget.

Possio har under hela vårt samarbete gett oss fria tyglar och låtit oss arbeta med frågor som verkligen intresserar oss. De har kommit med råd och tips men dessa har vuxit fram ur gemensamma diskussioner och deras förslag har därför aldrig känts begränsande. Detta har fått till följd att det inte har uppstått några intressekonflikter. Vidare har en medarbetare på Possio vid ett flertal tillfällen understrukit att det är viktigt att vi ex-jobbare ska skriva om ett ämne för vilket vi verkligen brinner, eftersom detta är en förutsättning för ett arbete med sådan kvalitet som Possio kräver.

Innan temaarbetet, vilket är en förberedande litteraturstudie för c-uppsatsen, inleddes var vi nybörjare på området Bluetooth respektive WLAN. Under de fem veckor som vi arbetade med temarapporten läste vi in oss på ämnet och skapade oss en god förståelse. VPN är däremot relativt nytt för oss och därför kommer vi att beskriva begreppet från grunden i denna uppsats. Enligt vår kännedom används VPN-lösningar med framgång vid distansuppkopplingar via Internet. Detta skulle kunna indikera att lösningen även skulle kunna passa vid trådlös kommunikation där mediet i likhet med Internet är osäkert.

En följd av vår positiva grundinställning till teknikutveckling är att vi ser integrering av WLAN och Bluetooth som något eftersträvänsvärt, då det leder till nya möjligheter för användaren.

Förutom detta icke valbara perspektiv har vi valt att angripa ämnet ur ett säkerhetsperspektiv. Detta beror på att säkerhet är ett ämne som intresserar oss. Vidare är det ett område där Possio efterfrågar hjälp med kunskapsinsamling samt råd till hur säkerheten kan förbättras i deras nya produkt.

Vi bygger vårt resonemang på att VPN eventuellt kan lösa säkerhetsriskerna i hela det integrerade Bluetooth- och WLAN-nätet. Detta skulle vara en fördel gentemot de säkerhetslösningar som är nätverksspecifika och alltså inte kan täcka ett helt integrerat nätverk.

2.1.1 Ordval

Denna uppsats riktar sig främst till personer som är kunniga inom IT-området. Därför har vi valt att inte att förklara, enligt vår mening, grundläggande IT-termer. Vidare har vi valt att inte översätta en del termer till svenska. Orsakerna till detta är flera. Exempelvis har vi inte alltid funnit någon bra svensk översättning och att försöka göra en på egen hand kan leda till att termen blir svårförståelig. Vidare anser vi att flera ord är mer eller mindre vedertagna begrepp, det vill säga att det engelska ordet har blivit ”svenskt”. Dessutom menar vi att den svenska översättningen kan göra att begreppet helt faller ur sitt sammanhang då ordet får en annan betydelse på svenska.

Exempel på ord och begrepp som vi valt att inte översätta är point-to-point, access point och Hotspot. Förhoppningsvis förenklar vårt ordval för läsaren och inte tvärtom.

2.1.2 Koppling till befintlig kunskap

Det finns relativt gott om litteratur och pålitliga Internetkällor som behandlar Bluetooth och WLAN. Vi har i huvudsak använt oss av fakta som återkom i flera av källorna och därför kan anses vedertagna.

Vi har inte funnit någon litteratur som berör integrerade trådlösa nätverk ur de aspekter vi har valt att behandla. Detta beroende på att tekniken inte finns på marknaden i dagsläget. Den information vi har tagit del av behandlar samexistens mellan de olika teknikerna och problem förknippade med detta.

Det finns litteratur och andra skriftliga källor, såsom Internet, som beskriver VPN. Inom detta område är inte utbudet av litteratur så stort men vi har dock funnit några böcker som behandlar olika delar av VPN. VPN-lösningar för trådlösa nätverk är nyare och detta är anledningen till att information om detta främst kan hittas på Internet. Eftersom underlaget är mindre har de enskilda källorna fått större inverkan än vid beskrivningen av Bluetooth och WLAN.

2.1.3 Centrala begrepp

Ett *nätverk* är två eller fler enheter som utbyter data med varandra.³²

Bluetooth är en trådlös radioteknik som stödjer både data- och röstöverföring.³³

Ett *WLAN* fungerar som ett LAN med undantaget att enheterna i nätverket kommunicerar via elektromagnetiska vågor istället för via kablage.³⁴

³² Mårild, K., Possio

³³ Miller, M., Discovering Bluetooth

³⁴ Cisco Systems

Förkortningen *VPN* står för *Virtuella Privata Nätverk* och är ett sätt tunnla information för att på ett säkert sätt överföra den över ett osäkert medium.³⁵

Med *integrerade trådlösa nätverk* avser vi i detta arbete trådlösa nätverk där Bluetooth och WLAN kopplats ihop med hjälp av gemensamma access points.

Vi använder orden *säkerhetsrisk*, *säkerhetslucka* och *säkerhetsproblem* synonymt. En risk kan i tekniska sammanhang definieras som ”sannolikheten för att en specificerad omständighet (riskkälla) leder till en specificerad oönskad händelse eller effekt under en angiven tidsperiod”³⁶. Begreppet säkerhetsrisk och dess synonymer innebär i denna uppsats en svaghet som kan utnyttjas av en inkräktare för att avlyssna eller göra intrång i nätverket.

Med *säkerhetsnivå* menar vi i denna uppsats grad av säkerhet, med andra ord om många eller få säkerhetsrisker är åtgärdade. Nivå betyder ursprungligen ”vågrät yta med visst höjdläge i förhållande till annan yta eller punkt”, betydelsen är ofta överförd med tonvikt på exempelvis kvalitet eller värde³⁷.

En *säkerhetslösning* eller en *säkerhetsåtgärd* betyder i denna uppsats en åtgärd mot en säkerhetsrisk, till exempel är ett dörrlås en säkerhetslösning mot inbrott. Lösning betyder ”lämplig åtgärd för att komma till rätta med praktiskt problem”³⁸.

En aspekt är ”ett av flera sätt att betrakta eller analysera någon företeelse till exempel ett problem eller en fråga”³⁹. En säkerhetsaspekt är alltså ett sätt att analysera säkerhet. Med *säkerhetsaspekter* avser vi i denna uppsats säkerhetsrisker samt säkerhetslösningar.

Säkerhetskriterier är sådana kriterier som måste uppfyllas för att ett nätverk ska anses vara säkert. Ett kriterium är ett avgörande kännetecken med vars hjälp det kan avgöras att ett visst villkor är uppfyllt⁴⁰.

2.2 Alternativa perspektiv

Säkerhet är ett mycket brett område liksom trådlösa nätverk vilket gör att det finns många tänkbara infallsvinklar inom området, såsom företagsekonomiskt perspektiv. Ett annat bakomliggande perspektiv skulle kunna få konsekvensen att andra delar av området utvecklats mer och aspekter som vi bortsett från skulle kunna ses som intressanta.

En företagsekonom skulle vara mer intresserad av att undersöka om huruvida säkerhetsbrister kan påverka ett företags lönsamhet. Tar sig en obehörig användare in i det lokala nätverket kan detta få ekonomiska konsekvenser för ett företag.

³⁵ Trudeau, P., Building Secure Wireless Local Area Networks

³⁶ Nationalencyklopedien

³⁷ Nationalencyklopedien

³⁸ Nationalencyklopedien

³⁹ Nationalencyklopedien

⁴⁰ Nationalencyklopedien

Vår utgångspunkt har varit att förklara så mycket om WLAN och Bluetooth som är nödvändigt för att kunna förstå de säkerhetsaspekter som är förknippade med teknikerna. När vi studerat VPN har vi på samma sätt fokuserat på de aspekter som är relevanta för integrerade Bluetooth- och WLAN-nät. Vilka aspekter vi valt att behandla präglas dels av vilken kunskap Possio är intresserad av samt våra egna förkunskaper. En annan uppsats med samma syfte skulle kunna innehålla långa avsnitt programkod eller matematiska beräkningar och skulle därför kunna bli mycket olik denna.

Ett alternativt perspektiv på vårt syfte är hur olika radiotekniker stör varandra. Det finns dock andra som undersöker detta.

Alternativa perspektiv skulle kunna leda till en uppsats som var mer inriktad på hur olika lösningar fungerar tekniskt och matematiskt, det går även att tänka sig en mer värderande inställning rangordnade olika VPN-lösningar.

Vi hade även kunnat jämföra olika VPN-lösningar med varandra men eftersom de flesta är utformade för att fungera över Internet och andra fysiska nätverk så är inte detta relevant för det resultat vi vill uppnå.

3 METOD

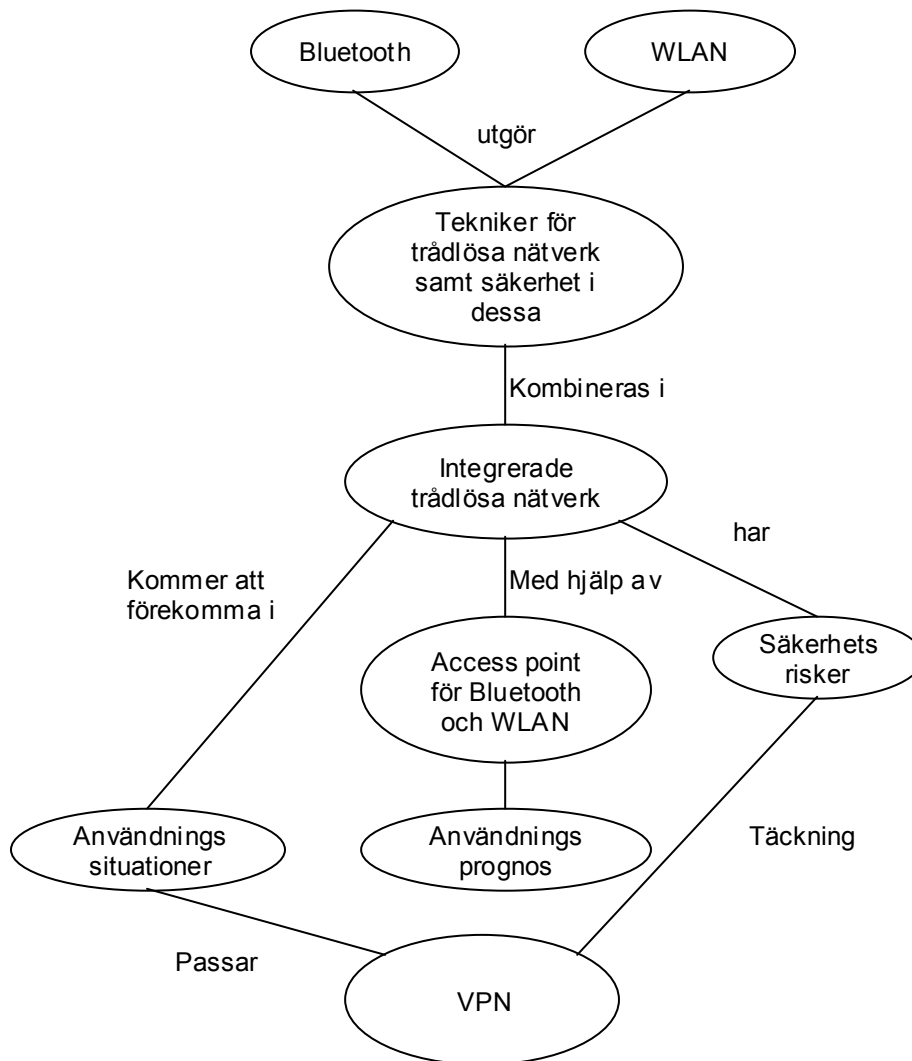
I detta kapitel ska vi beskriva vårt tillvägagångssätt, hur val av undersökningsobjekt har gått till och våra datainsamlingsmetoder. Vidare ska vi argumentera för våra val och utvärdera trovärdigheten samt tillförlitligheten i vårt arbete. Vi kommer även att beskriva alternativa metoder och motivera varför vi inte valt att använda oss av dessa.

En uppsats kan grundas på kvalitativa och/eller kvantitativa metoder. Kvalitativa metoder svarar på frågor såsom ”hur” och ”varför”. Kvantitativa metoder klarlägger mer statistiska samband och svarar på frågor som ”vad” och ”hur många”. I vår uppsats har vi integrerat de båda metoderna för att uppnå bästa möjliga resultat. Datainsamlingen och bearbetningen av material bygger till stor del på kvalitativ kunskap då vi har för avsikt att förklara begrepp och fenomen och ge både oss och läsaren en ökad förståelse för detta ämne. Vilka användningssituationer som är vanligast är en statistisk fråga och därför använder vi en kvantitativ metod i detta moment.

När data som samlas in med kvalitativ eller kvantitativ metod analyseras genereras kvalitativ kunskap. Detta eftersom den analysmetod vi använder är av kvalitativ art.

3.1 Tillvägagångssätt

Vi kommer först att beskriva vårt tillvägagångssätt översiktligt. I figur 1 ges en översiktsskild över hela tillvägagångssättet. De olika momenten beskrivs mer detaljerat i kommande delar av kapitlet.



Figur 1. Illustration av uppsatsens byggstenar och kopplingen mellan dessa. Egen figur.

Inför vårt temaarbete, vilket är en förberedelse inför c-uppsatsen, vände vi oss till en bekant på företaget Possio för att få tips på intressanta ämnesområden. Vi fick då förfrågan om att skriva uppsats i samarbete med företaget. Då våra intressen sammanföll med Possios inleddes ett samarbete.

I våra temarapporter skrev vi om WLAN respektive Bluetooth och därför föll det sig naturligt att i c-uppsatsen välja ett ämne som på något sätt behandlade de båda teknikerna. I samarbete med Possio kom vi fram till att vi skulle skriva om integreringen av de båda nätverksteknikerna med hjälp av access points och där avgränsa oss till säkerhetsaspekterna.

För att ta fram säkerhetskriterier som VPN måste uppfylla för att göra ett integrerat trådlöst nätverk säkert har vi beskrivit de tekniker som ingår (Bluetooth och WLAN) samt säkerhetsaspekter som existerar i de separata nätverksteknikerna. Vi har sedan jämfört och diskuterat säkerhetsaspekterna i de separata nätverksteknikerna för att komma fram till kriterier för säkerhet i integrerade trådlösa nätverk.

För att kunna bedöma hur väl olika VPN-lösningar passar i integrerade trådlösa nätverk ville vi veta i vilka situationer dessa kommer att användas. Olika typer av användning innebär olika typer av hårdvara med mera. För att få reda på vilka de vanligaste användningssituationerna var genomförde vi en enkätundersökning.

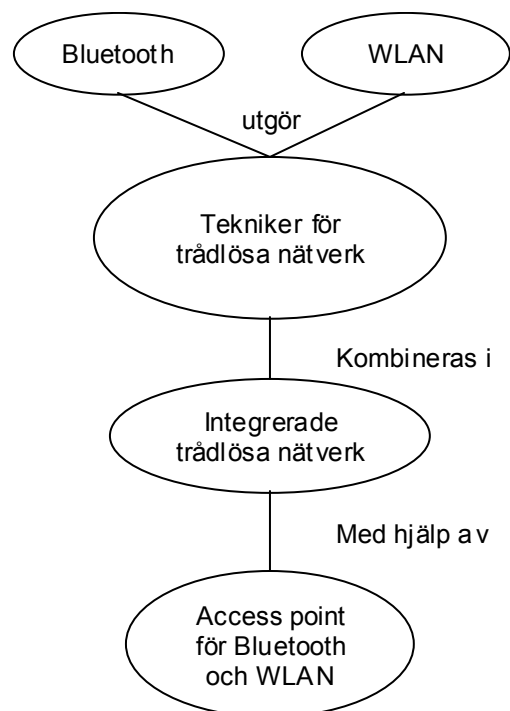
I vår analys formulerade vi säkerhetskriterier för integrerade trådlösa nätverk. Vi undersökte sedan hur väl VPN uppfyller dessa säkerhetskriterier. Därefter analyserade vi resultatet från vår enkätundersökning för att få en bild av de vanligaste användningssituationerna. Slutligen undersökte vi hur de olika tekniker som används i VPN-lösningar passar i dessa situationer.

3.1.1 Integrerade trådlösa nätverk

Med integrerade trådlösa nätverk menar vi i denna uppsats nätverk där teknikerna Bluetooth och WLAN samexisterar. Därför inleder vi med att beskriva teknikerna och jämför svaga och starka sidor hos de båda teknikerna. Utifrån detta har vi beskrivit varför det finns fördelar med att integrera teknikerna och hur detta tekniskt är möjligt. Dessutom beskrivs kortfattat hur integrerade trådlösa nätverk kan användas. Därefter har vi beskrivit säkerhetsrisker samt lösningar för de respektive teknikerna. I analysen använde vi sedan denna information för att formulera säkerhetskriterier för integrerade trådlösa nätverk.

Det som gör det möjligt att uppnå ett integrerat trådlöst nätverk är den produkt som Possio för närvarande utvecklar, PX20, som de kallar för en trådlös gateway. Denna fungerar som länk och tolk, alltså access point och gateway, mellan WLAN- och Bluetooth-nät. Denna access point kommer därför att utgöra en del av vår beskrivning av integrerade trådlösa nätverk. Att integrera dessa två typer av nätverk är något nytt. Säkerhetsaspekterna i integrerade trådlösa nätverk är därför i dagsläget outforskade.

Under kursens gång har vi regelbundet besökt Possio där vi träffat vår handledare samt eventuellt en eller flera medarbetare. Under dessa besök har vi under fria former diskuterat uppsatsen och fortsatt inriktning. Vi har även haft möjlighet att diskutera tekniska fenomen samt ställa frågor. Förutom dessa möten har vi skickat frågor via e-post till vår handledare på Possio vid behov.



Figur 2. Graföver beskrivning av integrerade trådlösa nätverk. Egen figur.

Till avsnitten om integrerade trådlösa nätverk har vi sökt information i litteratur från biblioteket och andra skriftliga källor främst på Internet. Vi har till stor del använt oss samma källor som till våra temaarbeten. Vad gäller fördelar med integrering av Bluetooth och WLAN har vi baserat oss på information från prognosföretaget Forrester samt Possio.

3.1.2 Virtuella Privata Nätverk

Det finns som vi nämnt tidigare säkerhetslösningar för WLAN och Bluetooth. Dessa arbetar på de lägsta skikten i OSI-modellen. Lösningarna för WLAN har dock kritiserats för att inte vara tillräckligt bra och vissa kritiker har framhållit VPN som ett tänkbart alternativ⁴¹.

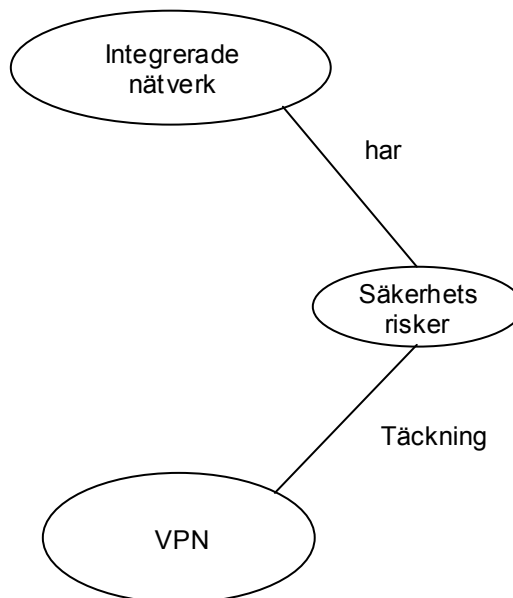
Av en teknikexpert på Possio fick vi förslaget att titta på VPN, vilket vi också gjorde. Detta beroende på att denna lösning borde kunna öka säkerheten och vara ett skydd nog för de säkerhetsrisker som existerar i integrerade trådlösa nätverk.

VPN omtalas ofta i tidningar som till exempel Computer Sweden, vilket har gett oss uppfattningen att VPN är en utbredd och accepterad lösning för fysiska nätverk.

Vi har beskrivit de aspekter av VPN som har med avlyssning och intrång att göra vad gäller VPN generellt. Vi har dessutom givit exempel från specifika VPN-lösningar. Detta för att få konkreta exempel på hur skydd mot avlyssning och intrång kan utformas. Denna beskrivning ligger till grund för analysen, där vi dels ställer VPN mot våra säkerhetskriterier, dels mot användningssituationer.

För att få information till den del som rör VPN har vi till största del använt oss av källor från Internet. De sökord vi har använt oss av är ”VPN”, ”Virtual Private Network” samt ”Virtuella privata nätverk”. Den sökmotor vi har använt är Altavista. Från medarbetare på Possio har vi även fått förslag på sidor där det finns relevant och läsvärd information.

Självklart hade vi helst använt oss av publicerad och tryckt litteratur, men denna har varit mycket svår att få tag på. Efter sökning i Örebro universitets katalog Voyager har vi endast funnit en uppsats, vilken är skriven på c-nivå. Vi har även sökt via Libris och där funnit en hel del böcker som finns att tillgå på andra universitetsbibliotek. De böcker vi funnit intressanta har vi fjärrlånat.

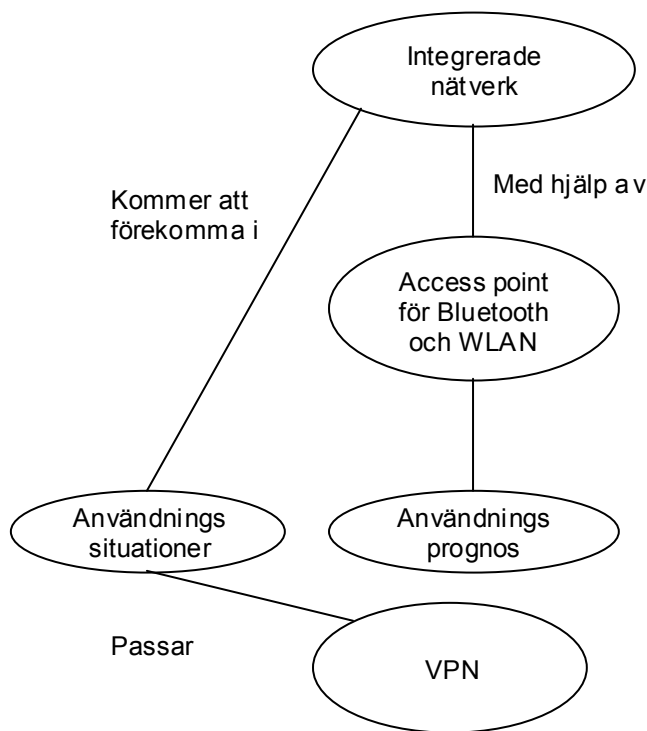


Figur 3. Graföver beskrivning av Virtuella Privata Nätverk. Egen figur.

⁴¹ Trudeau, P., Building Secure Wireless Local Area Networks

3.1.3 Användningssituationer

I analysen vill vi undersöka hur väl olika VPN-lösningar passar i de vanligaste användningssituationerna för integrerade trådlösa nätverk. Då det i dagsläget inte existerar några integrerade trådlösa nätverk valde vi att ta reda på i vilka situationer Bluetooth och WLAN används samt hur stort intresset är för att använda integrerade trådlösa nätverk. För att få reda på i vilka situationer integrerade trådlösa nätverk används har vi genomfört en enkätundersökning. Vi antog att om respondenterna ställde sig positiva till att använda integrerade trådlösa nätverk inom den närmsta framtiden så skulle användningssituationerna för Bluetooth och WLAN även gälla dessa integrerade trådlösa nätverk.



Figur 4. Graföver beskrivning av användningssituationer. Egen figur.

Enkäten bestod av fyra frågor samt möjlighet att fylla i övriga kommentarer (se bilaga). Vi genomförde ingen pilotenkät, då vi ansåg att frågorna var få och enkla. Vi ville inte få någon djupare förståelse utan endast se statistiska samband, därför föll valet av datainsamlingsmetod naturligt på enkätundersökning.

Vår avsikt var att få svar på var och när teknikerna WLAN och Bluetooth används. Vår uppsats behandlar en lösning som integrerar de båda teknikerna, men denna teknologi finns ännu inte på marknaden. Därför har vi ställt frågor som berör teknikerna var och en för sig. Det torde dock vara sannolikt att användningssituationerna som idag är vanligast för de respektive teknikerna även kommer att vara vanligast när teknologierna integreras. För att få en föräning om hur utbredd användningen av integrerade nätverk, där både WLAN och Bluetooth används, kommer att vara i framtiden formulerade vi även en fråga för detta.

De användningssituationer som vi lät respondenterna välja mellan i enkäten har vi tagit fram genom diskussioner med varandra utifrån våra egna kunskaper och information från Possio. De användningssituationer som vi genom diskussioner kom fram till var realistiska använde vi som svarsalternativ i enkäten. Vi lämnade även möjlighet för respondenten att fylla i ett eget svarsalternativ. Anledningen till att vi valde att ange så många alternativ var att underlätta för respondenten samt att förenkla sammanställningen av enkäten. Det öppna svarsalternativet tog vi med för att inte missa någon användningssituation. I efterhand kan vi dock konstatera att ytterst få respondenter använde det öppna svarsalternativet och av det drar vi slutsatsen att övriga svarsalternativ täckte de olika användningssituationerna.

Enkäten lades ut på Internet på sidan www.pellesoft.nu, vilken är ett forum för programmerare. Pelle Johansson, som är webmaster för denna sida, är en personlig bekant och han hjälpte oss att koda enkäten efter vår mall. När en respondent hade fyllt i svaren och tryckt på submit-knappen sändes svaren direkt till vår e-post.

Sidan www.pellesoft.nu är mycket välbesökt, cirka 800-1200 besökare per dag och programmeringsforumet har ungefär 5200 medlemmar.⁴² Besökarna är teknikintresserade och vi ansåg att detta var en bra möjlighet att komma i kontakt med så många användare som möjligt. Det slumpmässiga urvalet har vi bortsett ifrån, vi ville få in så många svar som vi kunde. Endast registrerade medlemmar i forumet kunde fylla i enkäten. Eftersom medlemmarnas uppgifter finns registrerade kunde vi skilja respondenterna åt med hjälp av deras e-postadresser som bifogades med svaren.

Vi skulle ha kunnat skicka ut enkäten till ett flertal företag som vi visste använde sig av WLAN eller Bluetooth. Denna metod valde vi dock bort eftersom det hade tagit lång tid att dels hitta företagen, dels att få in svaren. En annan möjlighet är att fråga människor på stan, men där kan det bli komplicerat att överhuvudtaget få tag på användare. Många studenter är teknikintresserade, vi valde dock bort denna grupp eftersom den trådlösa tekniken är relativt dyr att införskaffa och att detta hindrar studenter, som ofta har en skral ekonomi, från att använda den.

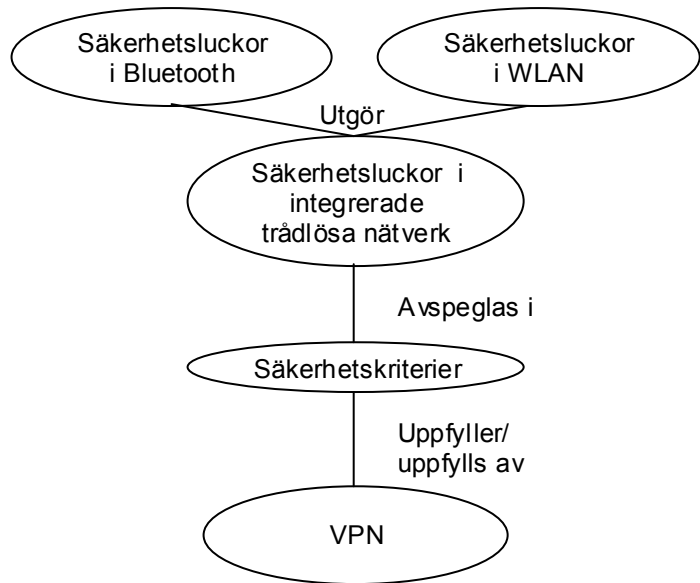
Uppgifter om användningsområden av trådlösa nätverk finns säkerligen att finna i någon tidskrift, men vi ansåg att vi ville ha de mest aktuella svaren. Vi valde därför att göra enkätundersökningen och på detta sätt kunde vi få svar på exakt de frågor vi hade.

Vår enkätundersökning var tillgänglig från fredagen den 23 november till söndagen den 2 december. Under denna tidsperiod fick vi in 86 svar. Av dessa har vi använt 75 stycken när vi sammanställt vår statistik. Att vi inte använt alla beror på att 7 stycken under rubriken övriga kommentarer angav att de inte använde sig av den trådlösa tekniken, dessa respondenter hade alltså inte läst den inledande texten, i vilken det tydligt framgår att enkäten vänder sig till Bluetooth- och/eller WLAN-användare. Vidare hade en person fyllt i enkäten 4 gånger. Detta framgick eftersom respondentens e-postadress bifogades vid varje svar. Sammanlagt användes inte 11 enkäter och detta gör att det externa bortfallet blev cirka 13 procent. Vi anser dock att 75 svar räcker för att vi ska kunna skapa oss en bild av användandet.

⁴² Johansson, P., forumet pellesoft

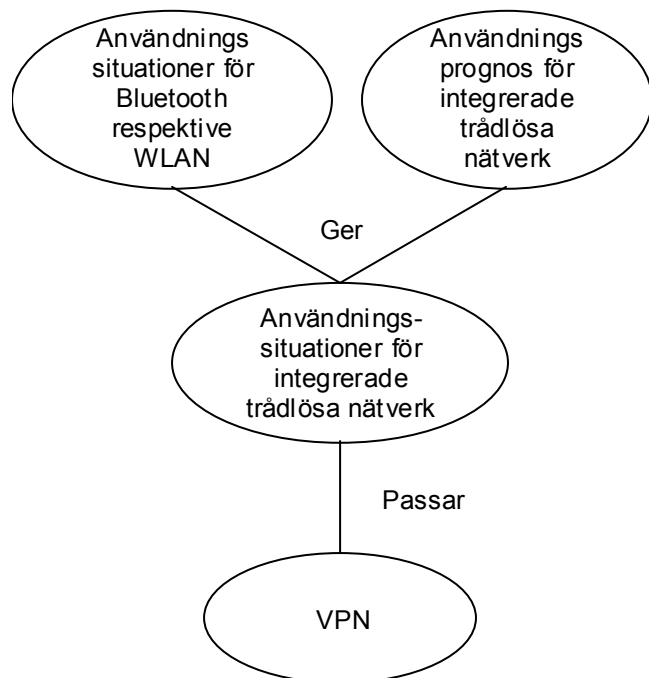
3.1.4 Analys

I den första delen av analysen jämför vi säkerhetsluckorna i Bluetooth- och WLAN-nät var för sig. Ur jämförelsen får vi de säkerhetsluckor som kommer att finnas i integrerade trådlösa nätverk. Detta gör att vi kan formulera säkerhetskriterier som måste uppfyllas för att göra ett integrerat trådlöst nätverk säkert. Säkerhetskriterierna ställs sedan mot VPN. På detta vis kan vi avgöra om VPN innehåller funktioner som uppfyller dessa säkerhetskriterier och därmed gör VPN till en möjlig säkerhetslösning för integrerade trådlösa nätverk.



Figur 5. Graföver beskrivning av analys, del 1. Egen figur.

I den andra delen av analysen tittar vi på vilka användningssituationer som visat sig vara vanligast för Bluetooth respektive WLAN. Om användarna till dessa tekniker är positiva till att använda integrerade trådlösa nätverk i framtiden så torde samma användningssituationer dominera i dessa nätverk. Därefter har vi analyserat hur väl olika VPN-lösningar passar i dessa situationer, både tekniskt och praktiskt. Vi tittar till exempel på vad som kan påverkas av mobilitet, utrymme och kapacitet.



Figur 6. Graföver beskrivning av analys, del 2. Egen figur.

3.2 Källkritik

Vår ambition var att låta information från litteratur ligga till grund för uppsatsen och sedan komplettera med källor från Internet samt primärdata. Litteratur är i allmänhet granskad i högre utsträckning än andra skriftliga källor och är därför bra att använda som bas. Eftersom detta område är så nytt, vissa saker vi skriver om finns knappt ännu, så var detta svårt. Därför kommer den största delen av sekundärdatan från Internet i vissa delar av uppsatsen, med detta i bakhuvudet har vi försökt vara extra kritiska och noga med att verifiera genom att undersöka flera källor.

På Internet är det svårt att vara säker på informationens äkthet, vem som har publicerat den och vad denna har för bakomliggande motiv. Vi har strävat efter att i så stor utsträckning som möjligt använda oss av information från kända företag, erkända forum eller författare. Exempel på detta är Cisco Systems och WLANA. Några webbsidor har vi även sökt upp efter tips från Possio, vilka vi har fullt förtroende för. Information från företag kan innehålla dold marknadsföring. Vi har haft detta i åtanke och valt att inte använda alltför vinklat material.

När en enkätundersökning genomförs är det alltid svårt att värdera hur pålitliga svaren är. Det är näst intill omöjligt att veta om respondenten svarar ärligt på alla frågor. I vår enkät finns dock inga känsliga och personliga frågor. Därför torde svaren till största del vara trovärdiga. Vi har även den uppfattningen att de personer som besöker www.pellesoft.nu är så mogna att de inte fyller i felaktiga svar i enkäten för att förstöra för oss i vårt uppsatsskrivande.

3.3 Validitet

Begreppet validitet innebär att författaren verkligen mäter det som hon avser att mäta.

Vi anser att det bästa sättet att skapa sig en bild av ett fenomen såsom Bluetooth, WLAN eller VPN är att studera litteratur och andra skriftliga källor, vilket vi har gjort. Ett alternativt tillvägagångssätt hade kunnat vara att samla information genom intervjuer, men eftersom vi endast är intresserade av objektiva fakta och inte åsikter så har vi valt bort detta tillvägagångssätt. Eftersom skriftliga källor tenderar att vara mer underbyggda och genomtänkta än muntliga tror vi att den metod vi valt ger den mest korrekta beskrivningen av fenomenet. Vi har även strävat efter att använda oss av så många källor som möjligt för att höja validiteten i uppsatsen.

Syftet är vidare att undersöka hur olika VPN-lösningar passar i de vanligaste användningssituationerna för Bluetooth- och WLAN-nät. För att få en rättvisande bild av vilka som är de vanligaste användningssituationerna utformade vi en enkät riktad till användare av Bluetooth eller WLAN. Enkäten innehöll fasta svarsalternativ kompletterat med möjlighet till öppna svar. Detta för att vara säkra på att vi inte utelämnat någon viktig användningssituation men samtidigt ha en enkät som var lätt att fylla i och sammanställa.

Vi använde 75 svar på enkäten. Ett större urval hade medfört högre validitet, då den statistiska säkerheten ökar med antal svar. Vi anser dock att 75 svar är tillräckligt eftersom vi endast ville skapa oss en uppfattning om framtiden och inte använda statistiken i bevisande syfte. Att vi nöjde oss med denna mängd svar har även påverkats av den begränsade tid vi har haft till vårt förfogande.

3.4 Reliabilitet

Denna uppsats är baserad på både kvalitativ och kvantitativ data. Om ett arbete har hög reliabilitet så innebär det att en annan person ska kunna följa samma metod och då komma fram till samma resultat. Detta är lättare att uppnå i en kvantitativ undersökning som till exempel den enkätundersökning som vi använt i denna uppsats än vid kvalitativ datainsamling.

För att få hög reliabilitet är det viktigt att beskriva metoden tydligt. För den kvalitativa delen av denna uppsats är även författarnas perspektiv av stor betydelse. Vi har försökt beskriva de delar av vårt perspektiv som har påverkat resultatet så tydligt som möjligt. Det är svårt att beskriva sitt perspektiv eftersom det till stor del är omedvetet, det har dock underlättat att vi är två personer som skriver uppsatsen tillsammans eftersom vi då kunnat diskutera med varandra och se värderingar och tankesätt hos den andra som är osynligt för en själv. En bra beskrivning av perspektiv är dock ingen garanti för att läsaren kan göra vårt perspektiv till sitt eftersom denne påverkas av sina referensramar. Denna uppsats vänder sig främst till teknikintresserade personer och detta höjer reliabiliteten eftersom de till viss del har referensramar liknande våra.

Vi har strävat efter att beskriva vårt tillvägagångssätt vid datainsamling av kvalitativ och kvantitativ data samt analys så tydligt som möjligt. Vi har bifogat enkäten som vi använde för att samla kvantitativ data. Vi har valt att lägga ut enkäten på ett webbforum för programmerare för att på ett enkelt sätt nå många teknikintresserade personer. Ju större urval desto fler enkätsvar och desto högre reliabilitet.

Reliabiliteten i vår uppsats höjs ytterligare i och med att vi har gjort noggranna källhänvisningar. Det är på så vis enkelt att kontrollera källorna.

4 INTEGRERADE TRÅDLÖSA NÄTVERK

I följande kapitel kommer vi inledningsvis att beskriva OSI-modellen och sedan de trådlösa teknikerna WLAN och Bluetooth. Vi beskriver teknikerna kortfattat för att ge en bild av hur de fungerar och varför de kompletterar varandra. Då teknikerna kompletterar varandra är en integrering av dem ett sätt att generera nya möjligheter för användaren. Integreringen kan ske med en access point, vilket vi kommer att beskriva. Denna access point finns ännu inte på marknaden men företaget Possio, vilka vi samarbetar med, lanserar sin access point PX20 i början av 2002.

I de separata nätverken WLAN och Bluetooth finns säkerhetsrisker men även lösningar. Dessa kommer vi att beskriva så att vi i analysen kan formulera säkerhetskriterier som bör uppfyllas för säkerhet i integrerade trådlösa nätverk, där både WLAN- och Bluetooth-enheter kan kommunicera med varandra. Vad gäller säkerhetsaspekterna har vi fokuserat oss på intrång i nätverket samt avlyssning.

4.1 OSI-modellen

För att lättare kunna förstå tekniken i trådlösa nätverk beskrivs här OSI-modellen kortfattat.

OSI står för Open Systems Interconnection.⁴³ Modellen togs fram av standardorganisationen ISO på 1980-talet och är ett ramverk som beskriver olika nivåer vid datakommunikation. Modellen är generell för alla typer av nätverk, skiktens utformning varierar sedan för olika typer av nätverk som till exempel Bluetooth- och WLAN-nät.

7	Applikationsskikt	Applikationer som använder nätverket
6	Presentationsskikt	Standardiserar data som används av applikationerna
5	Sessionsskikt	Handhar sessioner mellan applikationer
4	Transportskikt	Tillhandahåller felsökning och korrigerings
3	Nätverksskikt	Administrerar nätverksförbindelser. Adressering, vägval m.m.
2	Länkskikt	Har hand om dataöverföring över nätverket.
1	Fysiskt skikt	Definierar den fysiska överföringslänken

Figur 7. OSI-modellen. Källa: PCTechGuide, OSI Model

Det fysiska skiktet och länkskiktet har med nätverkskortet att göra, det är alltså endast dessa skikt som berörs av teknikerna Bluetooth och WLAN. Länkskiktet är indelat i två nivåer, Media Access Control (MAC) samt Logical Link Control (LLC). På MAC-nivån hanteras de olika accessmetoderna för lokala nätverk.⁴⁴ VPN kan dock arbeta på högre skikt. VPN kan till exempel byggas som en applikation och då således arbeta på skikt 7. Detta medför att applikationsutvecklaren måste ta hänsyn till säkerhetsaspekter som finns på lägre skikt i nätverket.⁴⁵

⁴³ PCTechGuide, OSI Model

⁴⁴ Ottosson, B., Internet & TCP/IP

⁴⁵ Quast, D.

4.2 Beskrivning av WLAN- och Bluetooth-teknikerna

WLAN

WLAN (Wireless Local Area Network) är ett trådlöst lokalt nätverk. Ett WLAN liknar ett fysiskt LAN med den stora skillnaden att informationsöverföringen i ett WLAN sker genom elektromagnetiska vågor, alltså i luften, istället för genom kablar som i ett fysiskt LAN.⁴⁶ I likhet med fysiskt LAN används IP-protokollet även i WLAN.⁴⁷

IEEE:s (Institute of Electrical and Electronics Engineers) standard 802.11 standardiserar signaler och protokoll i WLAN. WLAN använder tre olika fysiska implementeringar; infrarött ljus samt två tekniker för radiovågor.⁴⁸ Med radiovågor är maximalt avstånd mellan sändare och mottagare vanligen 50-100 meter⁴⁹. De flesta WLAN idag följer standarden 802.11b som är en utveckling av standarden 802.11.⁵⁰ Standarden 802.11b stödjer datahastigheter upp till 11 Mbs med hjälp av radiovågor.⁵¹ I standarden 802.11b används frekvensbandet 2.4 GHz. WLAN har en uteffekt på cirka 100 mW⁵².

WLAN-standardens 802.11 definierar topologierna BSS (Basic Server Set), IBSS (Independent Basic Server Set) och ESS (Extended Server Set)⁵³.

Topologin IBSS innebär att det trådlösa lokala nätverket är fristående⁵⁴.

I BSS-topologin kommunicerar varje station med en access point som förmedlar data till den mottagaren som kan vara en annan trådlös station eller en station i ett fysiskt nätverk. En access point kan sägas fungera som en ethernet-brygga.⁵⁵

Ett fysiskt LAN som kopplats ihop med flera BSS-nätverk via access points kallas Extended Service Set (ESS).⁵⁶

I standarden 802.11 definieras trådlösa stationer (STA) och access points (AP). En station är oftast en PC med ett nätverkskort (NIC) avsett för trådlösa nätverk men det kan även vara handdatorer och liknande med nätverkskort. Varje NIC identifieras av en 48 bits adress som kallas MAC-adress⁵⁷. En access point är en enhet som både kan sända och ta emot signaler och kopplar ihop trådlösa nätverk med varandra eller med fysiska nätverk.⁵⁸

⁴⁶ Cisco Systems

⁴⁷ Söderberg, U., Possio

⁴⁸ WLANA

⁴⁹ Jensen S m fl, Datakommunikation

⁵⁰ Geier, J., Wireless LANs

⁵¹ PCTechGuide, Wireless networks

⁵² Gilb, J., Mobilian

⁵³ Jensen S m fl, Datakommunikation

⁵⁴ WLANA

⁵⁵ Arbaugh, W A m. fl., Your 802.11 Wireless Network has No Clothes

⁵⁶ Jensen S m fl, Datakommunikation

⁵⁷ Jensen S m fl, Datakommunikation

⁵⁸ The linux-wlan Company

Bluetooth

Bluetooth är en teknik för att ersätta kablar på korta avstånd, till exempel mellan dator och tangentbord eller mobiltelefon och headset.⁵⁹ Kommunikationen mellan Bluetooth-enheter sker via radiovågor. Frekvensen som används är 2.4-2.48 GHz på det licensfria ISM-bandet (ISM står för Industrial, Medical, Science). Räckvidden på radiovågorna är cirka 10 meter då uteffekten endast är 1 mW. Detta får till följd att strömförbrukningen blir mycket låg.⁶⁰

Bluetooth-enheter kan vara sammankopplade i två typer av nätverkstopologier. Den vanligaste topologin kallas Piconet och i denna form av struktur kan upp till åtta enheter kommunicera. Kommunikationen sker antingen via point-to-point-koppling eller point-to-multipoint-koppling. Den enhet som först sänder ut signaler kallas master och det är även denna enhet som styr informationsöverföringen, de övriga enheterna kallas slavar.⁶¹

För att fler än åtta Bluetooth-enheter ska kunna kommunicera med varandra måste flera Piconets sammankopplas. Detta görs antingen genom att master-enheterna i respektive nät kopplas ihop eller att en slav blir en master i ett annat Piconet. Denna struktur av nätverk kallas scatternet. All kommunikation i detta nät filtreras genom master-enheterna. Det är möjligt att koppla samman tio Piconets, sammanlagt 80 olika Bluetooth-enheter.⁶²

I ett Bluetooth-nät kan både analoga meddelanden samt data överföras. Upp till 1 Mb data per sekund kan sändas, samt 64 kB analoga signaler per sekund på upp till tre kanaler.⁶³ Överföring av data i ett Bluetooth-nät sker i vissa fall med hjälp av IP-protokollet.⁶⁴

4.3 Integrering av Bluetooth och WLAN

	Bluetooth	802.11b WLAN
Primärt användningsområde	Ad hoc-nätverk mellan två enheter.	Komplement till LAN.
Maximal hastighet	1 Mbps	11 Mbps
Räckvidd	10 meter	50-100 meter
Dataöverföring	Ja	Ja
Ljudöverföring	Ja	Nej
Kräver separata access points (base stations)	Nej	I vissa fall
Energikrav	Låga	Höga
Kostnad att tillverka	Låga (cirka 150 kr, 2001)	Höga (cirka 1000-3000 kr, 2001)

Figur 8. Jämförelsegraf av 802.11 och Bluetooth. Källa: Miller, M., *Discovering Bluetooth*, Delvis omarbetad.

WLAN och Bluetooth är båda tekniker för trådlös dataöverföring men de konkurrerar inte nödvändigtvis med varandra. Intel meddelade på sitt utvecklarforum sommaren 2001 att

⁵⁹ Mårild, K., Possio

⁶⁰ Miller, M., *Discovering Bluetooth*

⁶¹ Communica Datadistribution AB

⁶² Miller, M., *Discovering Bluetooth*

⁶³ Communica Datadistribution AB

⁶⁴ Söderberg, U., Possio

802.11, alltså WLAN, blir defacto-standard för anslutning till Internet och att Bluetooth blir en nischprodukt⁶⁵.

Forrester är ett företag som analyserar teknologiska förändringar och hur det påverkar omgivningen. De menar att både WLAN och Bluetooth kommer att slå igenom i Europa. Företaget spår även att Bluetooth kommer att finnas i en mycket stor del av mobiltelefoner och handdatorer inom de närmsta åren, närmare bestämt 73 procent av mobiltelefonerna och 44 procent av alla handdatorer.⁶⁶

WLAN är överlägset Bluetooth vad gäller räckvidd, bandbredd och stöd för LAN standarder. Detta gör att WLAN är lämpligast för uppkoppling av laptops mot lokala eller publika nätverk och kommer att vara dominerande när det gäller Internetuppkoppling via access points på offentliga plaster såsom flygplatser och hotell.⁶⁷

Bluetooth passar däremot bättre för mobiltelefoner, handdatorer och andra mindre enheter. Bluetooth är billigare och strömsnålare än WLAN och stödjer dessutom röstöverföring i realtid. Forrester menar att Bluetooth kommer att dominera vad gäller kommunikation mellan telefoner, skrivare, handdatorer och scanners på kontoret samt mellan TV-apparater, videobandspelare med mera i hemmiljön.⁶⁸

Alltfler människor upptäcker fördelen med trådlösa nätverk. En trådlös uppkoppling möjliggör mobilitet på ett sätt som aldrig är möjligt med traditionella nätverk. Men vilken trådlös teknik är då bäst? Redan nu finns Hotspots där du kan koppla upp din WLAN-station mot ett WLAN via en access point. Via WLAN:et kan du sedan koppla upp dig mot Internet.⁶⁹ Ett WLAN har många av de fördelar som fysiska LAN har, det går att överföra data i relativt hög hastighet och signalerna når över ett område på 50-100 m⁷⁰, dessutom ger WLAN möjligheten till en flexiblare nätverksstruktur eftersom stationernas positioner inte är begränsade av kablar. Eftersom WLAN är en trådlös variant av ett fysiskt LAN är de två teknikerna kompatibla med varandra. Med denna utgångspunkt skulle dagens access points som kan koppla samman WLAN och fysiska nätverk vara tillräckliga för att ge mobila användare möjlighet att komma åt Internet eller ett företags fysiska lokala nätverk.

Vad är då en station? En station är en PC, en laptop, handdator eller kanske till och med en mobiltelefon som har ett nätverkskort för WLAN⁷¹. Problemet är att en WLAN-uppkoppling kräver så pass mycket energi att livslängden för ett batteri i en laptop, handdator eller mobiltelefon sänks kraftigt⁷². I en PC är detta inget problem eftersom datorn inte är batteridriven. För de övriga stationerna kan problemet med batteritiden lösas genom att stationen kopplas till ett strömuttag precis som en PC, men då förlorar stationen en del av sin mobilitet.

⁶⁵ Rittsel, P, Computer Sweden, nr. 113, 2001

⁶⁶ Forrester Research B. V.

⁶⁷ Forrester Research B. V.

⁶⁸ Forrester Research B. V.

⁶⁹ Sundman, M., Possio

⁷⁰ Jensen, S. m fl, Datakommunikation

⁷¹ The linux-wlan Company

⁷² Geier, J., Wireless LANs

Bluetooth är en teknik för trådlösa nätverk som kräver betydligt mindre energi än WLAN. Detta gör att Bluetooth passar bättre för batteridrivna mobila stationer som de vi nämnt ovan. Bluetooth-chip är dessutom billigare att tillverka än nätverkskort för WLAN. Dessa fördelar har gjort att allt fler mindre enheter som handdatorer och liknande i framtiden kommer att implementera Bluetooth. Bluetooth klarar dock inte att överföra data i högre hastigheter vilket gör att det inte är lämpligt som en ersättning av WLAN.⁷³

Detta ger oss följande situation. Det kommer att finnas en grupp användare med Bluetooth-enheter som kan användas för kommunikation mellan telefoner, skrivare, handdatorer med mera⁷⁴. Samtidigt finns det Hotspots där det går att koppla upp sig mot ett WLAN och via det vidare ut på Internet eller något annat fysiskt nätverk⁷⁵.

Både WLAN och Bluetooth har klara fördelar och nackdelar som gör att den ena tekniken inte kan ersätta den andra utan att de passar bäst i olika situationer. Bluetooth passar bäst i mobila sammanhang och WLAN i mer kapacitetskrävande sammanhang.⁷⁶ Det är här integrationen av de båda nätverkstyperna kommer in. Om en access point fungerar för båda dessa nätverkstyper kan denna placeras i en Hotspot och på så vis kan fördelarna från båda nätverkstyper kombineras. En mobil användare som har en handdator eller liknande med Bluetooth kan i en Hotspot av detta slag koppla upp sig mot det befintliga WLANet och vidare mot något annat fysiskt nätverk.⁷⁷

En access point kan sägas fungera som en ethernet brygga eftersom den kopplar ihop olika nätverk⁷⁸. Possio har utvecklat en trådlös access point som dessutom är en trådlös Gateway. Denna access point kombinerar Bluetooth och WLAN i en enda enhet. Med denna access point kan till exempel en enhet som implementerar Bluetooth kopplas ihop med en station i ett WLAN.⁷⁹

⁷³ Forrester Research B. V.

⁷⁴ Forrester Research B. V.

⁷⁵ Mårild, K., Possio

⁷⁶ Forrester Research B. V.

⁷⁷ Mårild, K., Possio

⁷⁸ Arbaugh, W. A. m fl, Your 802.11 Wireless Network has No Clothes

⁷⁹ www.possio.com



Figur 9. Access point för flera typer av trådlösa nätverk. Källa: Possio

Att Possios access point fungerar som en Gateway innebär att den kan översätta Bluetooth-signaler till WLAN och vice versa. Syftet är att en WISP (Wireless Internet Service Provider) ska installera denna access point i sin WLAN miljö för att möjliggöra för kunder att använda Bluetooth för att komma åt Internet. Denna access point, som heter PX20, finns inte till försäljning i dagsläget utan är i testfasen. Det finns enligt Possios kännedom ingen produkt med samma funktionalitet i en enda enhet på marknaden i dagsläget. Possio räknar med att släppa sin produkt i början av år 2002.⁸⁰

Det område som täcks av en access point kallas för Microcell. När en trådlös station kommer utanför en Microcell använder den sig av roaming. Detta innebär att stationen söker upp den access point som täcker det aktuella området.⁸¹ Zoner där det går att koppla upp sig mot WLAN, 802.11b, kallas även Hotspots.⁸²

4.4 Säkerhet

I följande underkapitel kommer vi att beskriva de säkerhetsaspekter som rör fenomenen intrång och avlyssning.

4.4.1 Vilka säkerhetsrisker föreligger för WLAN och Bluetooth?

Intrång

Att dessa tekniker är trådlösa och att radiovågorna kan ta sig genom en byggnads väggar gör att en inkräktare kan göra intrång i nätverk utan att upptäckas. Till skillnad från ett fysiskt nätverk behöver inkräktaren inte ha tillgång till ett fysiskt nätverksuttag för att få tillgång till nätverket.

⁸⁰ Mårild, K., Possio

⁸¹ WLANA

⁸² Ogelid, H., Computer Sweden, nr 111, 2001

En risk i ett WLAN är att någon tar sig in i nätverket och sänder data oavbrutet vilket leder till att alla andra stationer i nätverket står och väntar på sin tur. På detta vis kan ett helt nätverk blockeras.⁸³ När en access point blockeras på detta vis kallas det för en denial-of-service attack⁸⁴.

Även Bluetooth-nät kan utsättas för denial-of-service-attacker. När kontroll av behöriga enheter ska ske kan en enhet gå på gång skicka felaktiga värden till den andra enheten som denne måste kontrollera. När ett felaktigt värde mottas inträder en väntetid och systemet ligger nere.⁸⁵

Data i ett WLAN kan skyddas genom kryptering och det är då vanligt att en krypteringsnyckel lagras i hårdvaran vilket innebär att om någon stjälar hårdvaran så har denna full tillgång till nätverket.⁸⁶

Avlyssning

Största säkerhetsrisken i ett WLAN är det faktum att signalerna täcker ett stort område vilket gör det möjligt för en utomstående person att lyssna av datatrafiken till exempel utanför ett företags fysiska väggar.⁸⁷ Faktumet att Bluetooths radiovågor endast räcker 10 meter gör att det är säkrare än ett WLAN, men risk för avlyssning föreligger trots detta.⁸⁸

4.4.2 Lösningar

Åtgärder mot intrång

En åtgärd mot intrång är autentisering. Autentisering innebär att enheterna kontrollerar att de använder sig av samma hemliga nycklar. Detta bland annat för att ingen obehörig ska kunna koppla upp sig mot någon enhet där den kan komma åt hemlig information.⁸⁹

Eftersom WLAN fysiskt sett är mer oskyddade än fysiska LAN vad gäller obehörig åtkomst så innefattar 802.11 två autentiseringstjänster som kontrollerar åtkomst så att WLAN ska vara lika säkra som fysiska.⁹⁰

I WLAN-standarderna 802.11 definieras vissa tjänster för att förhindra att icke behöriga har tillgång till viss data samt att data som överförs endast kan tas emot och förstås av dem den är avsedd för. Dessa måste dock implementeras på alla stationer i ett WLAN vilket kan vara komplicerat i stora nätverk.⁹¹

För att förhindra att obehöriga tar sig in i WLANet kan en access point neka stationer utan rätt krypteringsnyckel tillträde⁹². Krypteringsfunktionen heter WEP (Wired Equivalent Privacy)⁹³.

⁸³ Geier, J., Wireless LANs

⁸⁴ Wavelink, Wireless Network Security – White Paper

⁸⁵ Persson, J. & Smeets, B., Bluetooth Security – an overview

⁸⁶ Cisco Systems

⁸⁷ Geier, J., Wireless LANs

⁸⁸ McDaid, C., Palowireless

⁸⁹ Persson, J. & Smeets, B., Bluetooth Security – an overview

⁹⁰ Geier, J., Wireless LANs

⁹¹ Cisco Systems

⁹² Cisco Systems

⁹³ Cisco Systems

En säkerhetsåtgärd för access points i ett WLAN är en Access Control List (ACL) vilket är en lista över alla stationer som är auktoriserade att använda nätverket. Listan innehåller stationernas MAC-adresser. En station som inte finns med på listan kan inte kommunicera med denna access point.⁹⁴

Ett problem är att MAC-adresser aldrig kodas, inte ens om krypteringsalgoritmen WEP används, och det går att ändra MAC-adress på ett nätverkskort med hjälp av särskild mjukvara. Detta gör att en inkräktare kan ta reda på en MAC-adress i ett nätverk som skyddas av ACL och sedan lura access pointen att släppa in inkräktaren.⁹⁵

Åtgärder mot avlyssning

Eftersom Bluetooths radiovågor endast sträcker sig 10 meter måste attackeraren vara fysiskt närvarande för att ha möjlighet att kunna göra intrång i systemet och kan följaktligen enkelt upptäckas.⁹⁶

Både WLAN och Bluetooth använder Spread spectrum-tekniker (SS) för att sända data. SS innebär att informationen som ska sändas delas upp över den tillgängliga bandbredden istället för att använda hela bandbredden som en kanal. Syftet med denna teknik är att signalen ska vara svår att avlyssna, förändra eller störa eftersom den liknar brus på grund av att signalen är utspridd över frekvensbandet.⁹⁷

De flesta WLAN använder en variant av SS som heter Direct Sequence Spread Spectrum (DSSS)⁹⁸. Denna teknik går ut på att all data som sänds är kodad genom att till synes slumpmässiga bitar blandas med data. Denna kodade data sänds sedan ut över hela det tillgängliga frekvensbandet.⁹⁹

Bluetooth använder en annan variant av SS som heter Frequency Hopping Spread Spectrum (FHSS). Som namnet antyder så innebär denna teknik att både sändare och mottagare hoppar mellan olika frekvenser. Det är endast den sändande och mottagande enheten som känner till det till synes slumpmässiga mönstret i hoppningen mellan frekvenserna.¹⁰⁰ Frekvenshoppningstekniken är inget heltäckande skydd mot avlyssning eftersom det är relativt enkelt för en obehörig med rätt utrustning att fånga upp radiosignalerna.¹⁰¹

Kryptering används för att förhindra att obehöriga kan tolka data som sänds i nätverket. I WLAN används krypteringsalgoritmen WEP. WEP är en symmetrisk krypteringsalgoritm där samma algoritm och nyckel används för både kryptering och dekryptering av data. Användare som saknar korrekt WEP-nyckel kan inte dekryptera data.¹⁰²

⁹⁴ Wavelink, Wireless Network Security

⁹⁵ Arbaugh, W. A. m fl, Your 802.11 Wireless Network has No Clothes

⁹⁶ McDaid, C., Palowireless

⁹⁷ Ewert, M., Datakommunikation

⁹⁸ Geier, J., Wireless LANs

⁹⁹ Ewert, M., Datakommunikation

¹⁰⁰ PCTechGuide, Wireless Networks

¹⁰¹ Persson, J. & Smeets, B., Bluetooth Security – An overview

¹⁰² Cisco Systems

Krypteringen i Bluetooth baseras på algoritmen SAFER+ (Secure And Fast Encryption Routine), en symmetrisk krypteringsalgoritm¹⁰³, som ändrar nyckeln vid varje överföring av data för att öka säkerheten. Genom att ändra nyckeln hindrar detta en obehörig som kommit över en krypteringsnyckel vid en överföring att använda denna för att dekryptera nästa session.¹⁰⁴ Nyckelns storlek kan variera mellan 8-128 bitar, detta beroende på att den ska följa varje lands olika restriktioner angående krypteringslängd.¹⁰⁵

¹⁰³ Kumria, A., University of Technology, Sydney

¹⁰⁴ Bray J. & Sturman C., Bluetooth – connect without cables

¹⁰⁵ Miller, M., Discovering Bluetooth

5 VIRTUELLA PRIVATA NÄTVERK

I följande kapitel kommer Virtuella Privata Nätverk (VPN) att beskrivas. Vi kommer dels beskriva hur det fungerar med autentisering, tunnling, kryptering samt brandväggar, men även visa några exempel på hur specifika VPN-lösningar kan se ut. Även vad gäller VPN fokuserar vi på fenomenen intrång och avlyssning, då vi har tittat på detta i integrerade trådlösa nätverk. Vi har lagt upp kapitlet på detta sätt eftersom vi i analysen vill kunna se om VPN uppfyller de kriterier för säkerhet som vi kommer att ställa upp. Vi tar även upp exempel på praktiska lösningar för att kunna analysera hur VPN passar i olika användningssituationer.

5.1 Inledning

VPN är ett Virtuellt Privat Nätverk som använder ett publikt nätverk, exempelvis Internet, för att koppla ihop två datorer som ett nätverk. Istället för att använda fysiska uppkopplingar som till exempel hyrda linor använder sig VPN av virtuella uppkopplingar såsom routing via Internet från ett företags privata nätverk till en anställds privata dator.¹⁰⁶

Ett privat nätverk är i allmänhet ett nätverk som tjänar ett visst syfte, såsom e-post, schemaläggning med mera, för en viss grupp människor. En viktig aspekt av ett privat nätverk är att det vanligtvis finns en viss grad av säkerhet i nätverket just för att det är privat. Säkerheten i det privata ligger i att det är svårt att komma åt nätverket rent fysiskt, det kan exempelvis inrymmas i ett företags kontor. En annan aspekt hos privata nätverk är att det centralt går att kontrollera vilka som har tillgång till nätverket. Det som skiljer ett privat nät från ett publikt är att i ett publikt nätverk har alla tillgång till nätet och det finns ingen specifik ägare till detta.¹⁰⁷

Att någonting är virtuellt innebär att vissa egenskaper simuleras. I VPN ligger det virtuella i att det är ett nätverk som simulerar några av de egenskaper som finns i ett privat nätverk. Kontentan av detta är att VPN existerar över ett publikt nätverk men samtidigt ändå tillhandahåller några av de egenskaper som finns hos privata nätverk.¹⁰⁸

VPN innehåller krypteringstjänster för att skydda data som transporteras över ett publikt nätverk. Denna krypteringstjänst ger den säkerhet mot avlyssning som ett vanligt privat nätverk får genom den fysiska säkerheten i nätet.¹⁰⁹

VPN är ett virtuellt nätverk och alltså inget fysiskt nätverk. Strukturen hos ett VPN-nät behöver inte vara statisk eftersom nätverkets struktur byggs upp av de stationer som ingår i VPN-nätet.¹¹⁰ I ett VPN används endast dynamiska uppkopplingar, inte statiska. Nätverksstrukturen skapas när en enhet ber om att få upprätta kontakt med en annan enhet. När kontakten sedan bryts existerar inget nätverk.¹¹¹ Användarna i ett VPN kan uppleva nätverket som lokalt trots att det inte är uppbyggt så rent fysiskt.¹¹²

¹⁰⁶ Tyson, J., How Virtual Private Networks Work

¹⁰⁷ Shea, R., L2PT – Implementation and operation

¹⁰⁸ Shea, R., L2PT – Implementation and operation

¹⁰⁹ Shea, R., L2PT – Implementation and operation

¹¹⁰ Microsoft, Virtual Private Networking: an overview - White Paper

¹¹¹ Kosiur, D., Building and Managing Virtual Private Networks

¹¹² Microsoft, Virtual Private Networking: an overview, White Paper

VPN är alltså en lösning för att på ett säkert sätt kunna överföra data över ett osäkert medium¹¹³.

VPN kan vara mjukvaru- eller hårdvarubaserade. En del mjukvarubaserade lösningar kräver en server i botten, andra inte.¹¹⁴

5.2 Typer av VPN

Det finns tre vanliga typer av VPN; Remote Access, Intranetbaserade och Extranetbaserade.

Remote Access: Även kallad VPDN (Virtual Private Dial-up Network). Denna uppkoppling sker mellan användare och LAN och används då exempelvis en anställd vill koppla upp sig mot företagets LAN men befinner sig på en annan plats. Vanligtvis outsourcar företaget VPN-tjänsten till en Enterprise Service Provider (ESP), vilken sätter upp en Network Access Server (NAS) som tillhandahåller mjukvara till användarnas datorer. Användarna kan ringa ett nummer för att nå en NAS och på det sättet få tillgång till företagets nätverk.

Exempel på företag som använder denna typ av VPN är stora företag med hundratals säljare på fältet. Remote Access VPNs medger säkra, krypterade uppkopplingar mellan företags privata nätverk och fjärranvändare med hjälp av en tredje part som tillhandahåller tjänsten. Det är denna typ av VPN som används när en användare kopplar upp sig över Internet.¹¹⁵

Intranetbaserade: Har företaget flera avdelningar på olika platser och ändå vill använda sig av samma privata nätverk kan de skapa ett Intranet-VPN för att koppla ihop ett LAN med ett annat.¹¹⁶

Extranetbaserade: Samarbetar ett företag nära med ett annat företag (till exempel en leverantör eller kund) kan ett Extranet byggas som kopplar ihop de olika företagens LAN.¹¹⁷

5.3 VPN-säkerhet¹¹⁸

VPN kan använda flera olika metoder för att säkra uppkoppling och data. Dessa metoder kan användas oavsett VPN-typ.

5.3.1 Brandväggar

En brandvägg tillhandahåller en stark barriär mellan ett privat nätverk och Internet. Brandväggen begränsar antalet portar där data får passera, den kontrollerar även vilka paket som passerar och avgör vilka protokoll som är tillåtna. Vissa VPN-lösningar inkluderar brandväggsfunktioner.

¹¹³ Trudeau P., Building Secure Wireless Local Area Networks

¹¹⁴ Andersson, N., Säkerhet och sekretess, nr 4, 2001

¹¹⁵ Tyson, J., How Virtual Private Networks Work

¹¹⁶ Tyson, J., How Virtual Private Networks Work

¹¹⁷ Tyson, J., How Virtual Private Networks Work

¹¹⁸ Tyson, J., How Virtual Private Networks Work

5.3.2 Autentisering

Det finns VPN-lösningar för att skydda känsliga applikationsservrar genom att begränsa åtkomsten på olika sätt. En icke-auktoriserad person ska inte kunna skicka några datapaket till en sådan server.¹¹⁹

I en VPN-lösning är det användarens identitet och inte klientens IP-adress som avgör vilka tjänster som ska vara tillgängliga. Det går även att använda ytterligare regler som reglerar användandet av en viss tjänst till vissa dagar och vissa tider för olika typer av användare.¹²⁰

AAA-servers (Autentisering, authorization, accounting) används för en säkrare uppkoppling i en Remote Access VPN-miljö. När en förfrågan om en uppkoppling kommer från en klient, behandlas frågan av denna server. AAA kontrollerar följande;

- Vem användaren är (Autentisering)
- Vad användaren är tillåten att göra (Authorization/attestering)
- Vad användaren verkligen gör (Accounting/redogörelse)¹²¹

När en inkräktare utger sig för att vara en legitim användare kallas detta spoofing. När en ny uppkoppling initieras kontrollerar klienten serverns identitet för att utesluta spoofing. När användaren sedan har blivit autentiserad skapas en säker krypterad tunnel.¹²²

5.3.2.1 Autentiseringsmetoder

En användare kan autentiseras med hjälp av ett enkelt lösenord. Detta är den minst säkra autentiseringsmetoden eftersom samma lösenord används upprepade gånger. Om någon obehörig får tag på lösenordet finns det ingen möjlighet för servern att skilja denna person från den behöriga användaren. Lösenorden skickas dock i en krypterad tunnel för att de inte ska vara synliga för övriga nätverket.¹²³

En något säkrare metod är att använda engångslösenord som kan genereras av någon form av dosa eller kort som visar ett nytt unikt lösenord för varje användningstillfälle.¹²⁴

Certifikat blir allt populärare att använda. I certifikat används digitala signaturer. Certifikatet innehåller oftast användarnamn, en privat nyckel samt utgivarens namn och den publika nyckeln. Ett certifikat kan vara en lösenordsskyddad fil på en dator eller så kan det lagras på ett smart card. Om certifikatet lagras som en lösenordsskyddad fil är det bara aningen säkrare än att använda ett enkelt lösenord.¹²⁵

En annan mycket säker autentiseringsmetod är biometrisk autentisering.¹²⁶ Autentiseringen sker då med hjälp av exempelvis fingeravtryck eller scanning av ögats hornhinna.

¹¹⁹ AppGate White Paper

¹²⁰ AppGate White Paper

¹²¹ Tyson, J., How Virtual Private Networks Work

¹²² AppGate White Paper

¹²³ AppGate White Paper

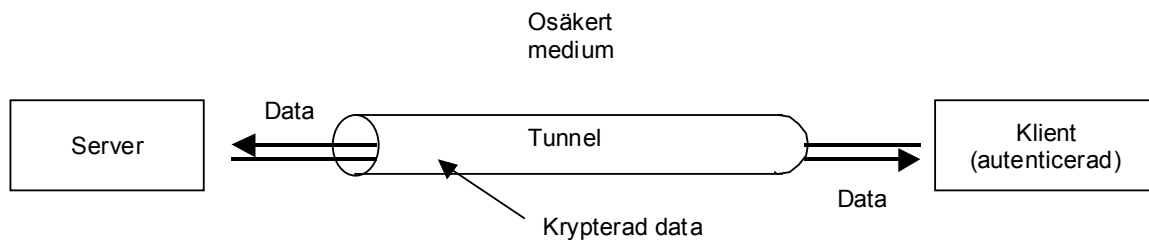
¹²⁴ AppGate White Paper

¹²⁵ AppGate White Paper

¹²⁶ Lawton, G., Lock up your Wireless LAN

5.3.3 Tunnling

De flesta VPN-lösningar använder tunnling för att skapa ett privat nätverk som når över Internet. När tunnling används packas ett helt paket in i ett annat paket och detta sänds över nätverket. Det yttersta paketets protokoll förstås av nätverket samt båda punkter (tunnel interfaces) där paketen går in och går ut (enter/exit).¹²⁷ Ordet tunnling kommer från ordet tunnel och en VPN-tunnel kan liknas vid en vanlig biltunnel. Någon som befinner sig utanför tunneln kan inte se vad som finns inuti den.



Figur 10. Illustration av tunnling. Egen figur.

Tunnling kräver tre olika protokoll:

- **Bärarprotokoll:** Protokollet som används av nätverket informationen färdas över.
- **Inkapslingsprotokoll:** Protokollet som originaldatan paketeras i. (GRE, Ipsec, L2F, PPTP, L2TP).
- **Passagerarprotokoll:** Originaldatan som blir överförd.

Med hjälp av tunnling kan ett paket, som använder ett protokoll som inte stöds av till exempel Internet, skickas i ett IP-paket och säkert sända detta via Internet. Det går även att skicka ett paket som använder en privat IP-adress inuti ett paket som använder en global unik IP-adress för att utöka det privata nätverket över Internet.¹²⁸

Tunnlingen kan dock inte ge exakt samma egenskaper som hos ett privat nätverk. Det är till exempel svårt att hemlighöja mängden data som trafikerar nätverket. Dessutom kan det gå att förstå vilken typ av applikation som används genom att iaktta storleken på paketet och när de sänds.¹²⁹

5.3.3.1 IPSec

IPSec (Internet Protocol Security Protocol) är ett inkapslingsprotokoll som tillhandahåller egenskaper för förhöjd säkerhet och är det vanligaste inkapslingsprotokollet som används i VPN-lösningar. IPSec har två krypteringslägen, tunnel och transport. I tunnelläget krypteras huvudet och innehållet, denna metod kallas Encapsulation Security Payload (ESP). I transportläget krypteras endast innehållet.¹³⁰

¹²⁷ Tyson, J., How Virtual Private Networks Work

¹²⁸ Tyson, J., How Virtual Private Networks Work

¹²⁹ Shea, R., L2PT – Implementation and operation

¹³⁰ Tyson, J., How Virtual Private Networks Work

IPSec-protokollet tillhandahåller tre funktioner:¹³¹

1. Identifiering av båda parter
2. Håller informationen konfidentiell
3. Ser till att informationen inte har ändrats under transport av tredje part

IPSec består av flera underliggande protokoll; IKE, ESP (se ovan) samt AH och är egentligen ett ramverk. Protokollet Internet Key Exchange (IKE), vilket förhandlar om hur trafiken ska skyddas.¹³² Protokollet Authentication Header (AH) fastställer användarens identitet¹³³. Metoden ESP använder krypteringsalgoritmen 3des för att kryptera trafiken¹³⁴. 3des är en symmetrisk krypteringsalgoritm¹³⁵ (se avsnitt 5.3.4 Kryptering).

5.3.3.2 Exempel på upprättande av tunnel mellan server och klient

Om en användare vill använda en tjänst på en skyddad server så startar användaren en programvara som upprättar en krypterad tunnel mellan klienten och servern. Om användaren blir autentiserad kontrollerar servern i en databas vad den specifika användaren ska ha tillgång till för tjänster. Beslutet baseras på användarens identitet, det aktuella klockslaget och veckodagen samt klientens IP-adress. I databasen kan det till exempel finnas regler som säger att användare inom företaget bara behöver ett lösenord för att bli godkända medan distansanvändare behöver ett smart card.¹³⁶

I nästa skede blir klienten informerad om vilka tjänster som finns tillgängliga. Dessa presenteras för användaren i ett grafiskt användargränssnitt där användaren kan välja applikation genom att klicka på en ikon. När en applikation har valts av användaren skickas en förfrågan till servern som loggar förfrågan, kontrollerar databasen igen och sedan släpper igenom trafiken om informationen från databasen medgav det.¹³⁷

VPN-mjukvaran hos klienten ber bara servern om tillgång till den eller de tjänster som behövs vid varje tillfälle. Om en användare till exempel vill läsa sin e-post kommer ingen datatrafik som inte är förknippad med detta att tillåtas. Fördelen med detta är att om någon obehörig person får tillgång till en uppkopplad klient så får inkräktaren endast tillgång till den tjänst som är igång för tillfället. Dessutom går det via en loggfunktion att se exakt vilken användare som hade tillgång till en viss tjänst vid en specifik tidpunkt.¹³⁸

5.3.4 Kryptering

Kryptering kodar data så att endast användaren, för vilken datan är avsedd för, kan läsa den. De flesta krypteringssystem tillhör en av följande två kategorier.

- Symmetrisk kryptering
- Asymmetrisk kryptering

¹³¹ Ricknäs, M., Computer Sweden, 2001-11-02

¹³² Ricknäs, M., Computer Sweden, 2001-11-02

¹³³ Bodin, P., Nätverk och Kommunikation, nr 18, 2001

¹³⁴ Ricknäs, M., Computer Sweden, 2001-11-02

¹³⁵ OpenBSD

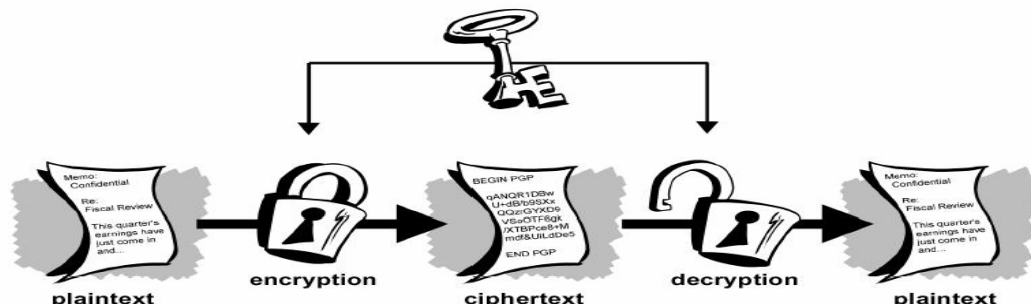
¹³⁶ AppGate White Paper

¹³⁷ AppGate White Paper

¹³⁸ AppGate White Paper

Symmetrisk kryptering¹³⁹

Symmetrisk kryptering innebär att avsändaren till ett meddelande krypterar meddelandet med en nyckel och mottagaren dekrypterar meddelandet med samma nyckel.



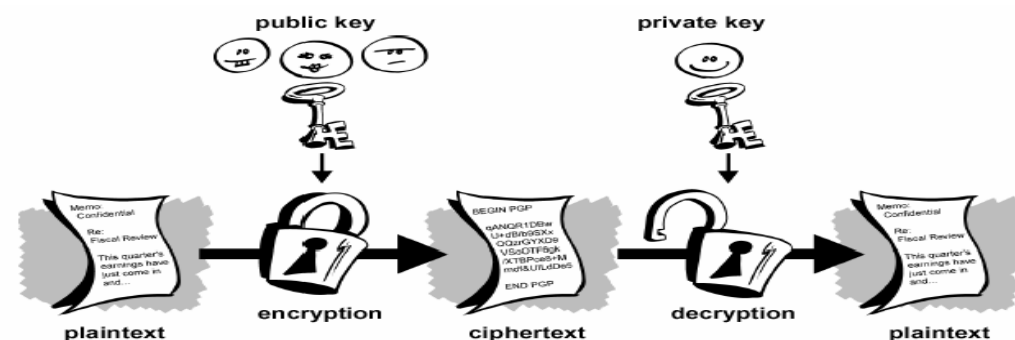
Figur 11. Symmetrisk kryptering. Källa: Introduction to Cryptography, User's Guide PGP 7.0.

Ett stort problem med symmetrisk kryptering är hur både avsändaren och mottagaren ska ha tillgång till samma nyckel, för att skicka nyckeln krävs en säker överföring så varför inte skicka meddelandet på samma sätt från början? Ett sätt att lösa detta är att överlämna nyckeln personligen. Om personen skulle bli av med nyckeln på vägen får avsändaren reda på detta och använder således inte de nycklar som skickats med kuriren.

Fördelen med symmetrisk kryptering är att den är relativt säker och kräver inte så mycket CPU-kraft.

Asymmetrisk kryptering

Asymmetrisk kryptering innebär att varje person har två nycklar, en publik för kryptering och en privat för dekryptering¹⁴⁰



Figur 12. Asymmetrisk kryptering. Källa: Introduction to Cryptography, User's Guide PGP 7.0.

En stor fördel med asymmetrisk kryptering i jämförelse med symmetrisk är att den publika nyckeln är just publik, med andra ord tillgänglig för alla. Användarna undviker på så sätt problemen med nyckeldistributionen.¹⁴¹

¹³⁹ Garfinkel, S., PGP Pretty Good Privacy

¹⁴⁰ Singh, S., Kodboken

¹⁴¹ Singh, S., Kodboken

5.4 VPN i trådlösa nätverk¹⁴²

Användningen av trådlösa nätverk ökar. Detta kommer ur behovet av att ha åtkomst till företagsinformation oberoende av var användaren befinner sig eller vilken utrustning hon har.

TCP/IP skapades när datakommunikation främst skedde mellan stationära datorer i fysiska nätverk. Trots att mycket har förändrats och mobila användare och trådlösa nätverk blir allt vanligare så har TCP/IP utvecklats på samma sätt.

VPN är en metod för företag som vill ha åtkomst till privata tillgångar över publika nätverk på ett säkert sätt. VPN är ett steg mot mobilitet för information, dagens teknik har dock brister när det kommer till trådlös datakommunikation.

De flesta VPN-lösningar som finns i dagsläget är designade för fysiska nätverk. Vissa av dessa fungerar även i trådlösa nätverk¹⁴³. Det finns även en VPN-lösning som är speciellt anpassad för att ta vara på de fördelar som finns med trådlösa nätverk.

Att sända data i ett trådlöst nätverk för vanligtvis med sig problem som lite bandbredd, dålig stabilitet i uppkopplingen samt oberäknelig tillgång till nätverket. Dessa problem kan lösas av en VPN-lösning för trådlösa nätverk så att lösningen ska bli pålitlig och användbar.

Vad gäller VPN för fysiska nätverk har det argumenterats för att de bör byggas på IP-nivå, det vill säga på nätverksskiktet i OSI-modellen, för att uppnå högsta möjliga transparens för användare och applikationer. Problemet är att många av de problem som finns i trådlösa nätverk inte kan lösas i nätverksskiktet. Transparens och enkelhet är dock viktiga egenskaper hos VPN vilket medför att en VPN-lösning för trådlösa nätverk också måste ha dessa egenskaper.

Säkerheten i VPN är av avgörande betydelse, både för fysiska och trådlösa nätverk. Därför bör VPN-lösningen integreras med brandväggar och andra tänkbara säkerhetsåtgärder som redan är implementerade i nätverket.

Säkerheten och transparensen kan uppnås med VPN på IP-nivå, men problemen med bandbredd och kvalitet på uppkoppling kan inte lösas på detta vis. För att åtgärda detta krävs ytterligare mjukvara vilket kan försvåra administrationen av ett sådant system. Det går dock att åtgärda problemet på ett annat sätt, nämligen genom att skapa en VPN-struktur som stödjer kommunikation i både trådlösa och fysiska nätverk.

I framtiden är det troligt att det kommer att finnas ett antal olika typer av trådlösa nätverkstyper som knyts ihop i Hotspots. WLAN och Bluetooth tillhandahåller dataöverföring till hög hastighet inom dessa områden medan mobila nätverk som 3G endast används utanför områdena.

¹⁴² Columbitech, WVPN White Paper

¹⁴³ Thoresson, A., AppGate

5.5 Speciella egenskaper hos en VPN-lösning anpassad särskilt för trådlösa nätverk¹⁴⁴

Det finns flera VPN-lösningar som fungerar i både trådlösa och fysiska nätverk. Det finns en lösning som är speciellt anpassad för trådlösa nätverk och därför har ett antal extra funktioner.

I denna lösning baseras de säkerhetsfunktioner som arbetar på transport- och nätverksskiktet på PKI. PKI (Public Key Infrastructure) är ett system som krypterar och autentiserar överföring av data¹⁴⁵. Lösningen är mjukvarubaserad och är tänkt att vara ett komplement till existerande kommunikationsinfrastruktur snarare än en ersättning.

För att fungera särskilt väl i trådlösa nätverk komprimerar denna VPN-lösning data innan den krypteras.

För att avbrott i uppkopplingen inte skall märkas finns funktioner för återupptagande av en avbruten session samt mekanismer för återställande av transaktioner (transaction recovery). Det första behövs eftersom en session kan blockeras under perioder då nätverket är otillgängligt för att sedan kunna fortsätta när radiovågorna kan nå mottagaren igen. Mekanismerna för återställande av transaktioner gör att applikationer kan återuppta dataöverföringen från det läge där överföringen avbröts utan att redan sänd data behöver skickas igen. Säkerhetsåtgärderna fungerar både över trådlösa och fysiska nätverk.

Lösningen är avsedd för en miljö bestående av både publika mobila nätverk och lokala trådlösa Hotspots och innehåller stöd för roaming mellan olika typer av trådlösa nätverk. Till exempel kan en mobil användare bibehålla en säker trådlös uppkoppling från en Hotspot på en flygplats där Bluetooth används vidare i en taxi där ett offentligt mobilnät används och slutligen i WLAN-nätet på sitt företag, hela denna förflyttning ska alltså kunna ske utan att uppkopplingen bryts och utan att användaren behöver logga in på nytt.

¹⁴⁴ Columbitech, WVPN Product Sheet

¹⁴⁵ Lindqvist, J., Nätverk och Kommunikation, nr 18, 2001

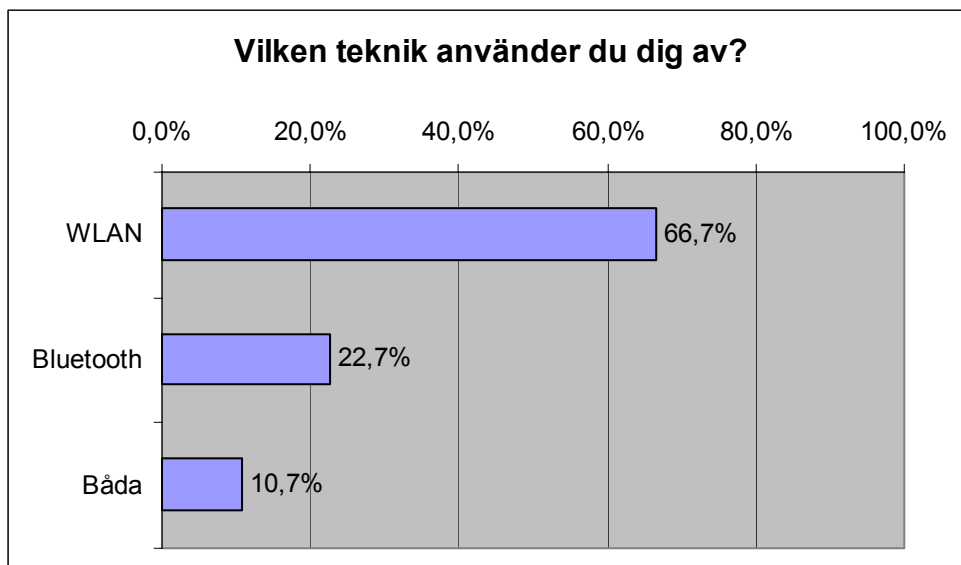
6 ANVÄNDNINGSSITUATIONER

I detta kapitel kommer vi att presentera resultaten från vår enkätundersökning (se även bilaga 1). Vi genomförde vår enkätundersökning eftersom vi ville få reda på de vanligaste användningssituationerna för de trådlösa teknikerna. Då det i dagsläget ännu inte finns någon fungerande lösning för integrering av de båda teknikerna ställde vi frågor som berörde de båda teknikerna separat. För att få en föräning om huruvida respondenterna i framtiden kommer att använda sig av integrerade trådlösa nätverk ställde vi även en fråga om detta. Vi har gjort antagandet att om respondenterna ställer sig positiva till att använda integrerade trådlösa nätverk inom en snar framtid så kommer samma användningssituationer dominera i dessa nätverk som för de separata teknikerna i dagsläget.

Enkätundersökningen genomfördes för att utröna vilka de vanligaste användningssituationerna var. Detta gjorde vi för att sedan kunna undersöka hur olika VPN-lösningar passar i dessa situationer, rent tekniskt och praktiskt.

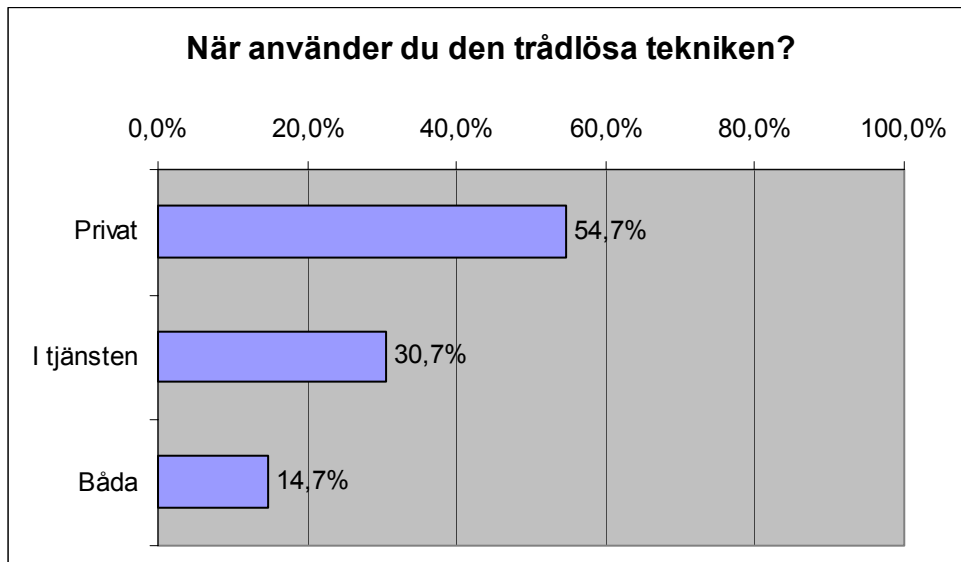
6.1 Vilka användningssituationer är vanligast?

En majoritet 66,7 procent (50 stycken) av respondenterna använder enbart WLAN. 22,7 procent (17 stycken) använder istället Bluetooth och 10,7 procent (8 stycken) använder sig av båda teknikerna.



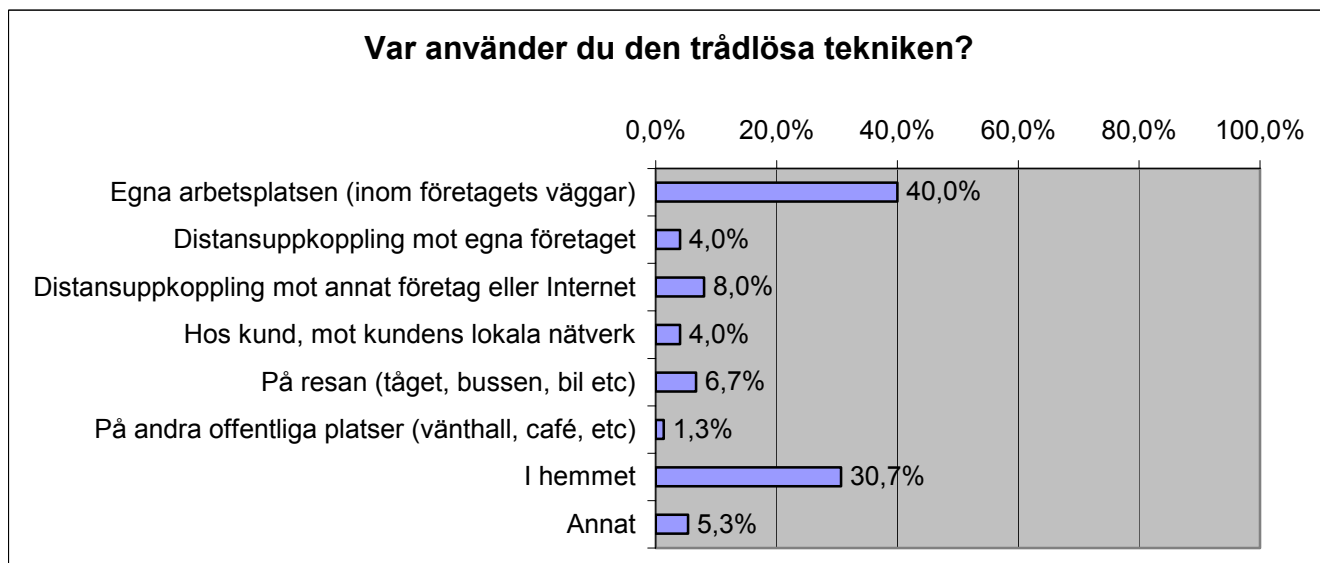
Figur 13. Fråga 1. Egen figur.

Till största del används den trådlösa tekniken i privat syfte. Det var 54,7 procent (41 stycken) som valde detta svarsalternativ. 30,7 procent (23 stycken) använde tekniken endast i tjänsten. 14,7 procent (11 stycken) av respondenterna använder båda teknikerna.



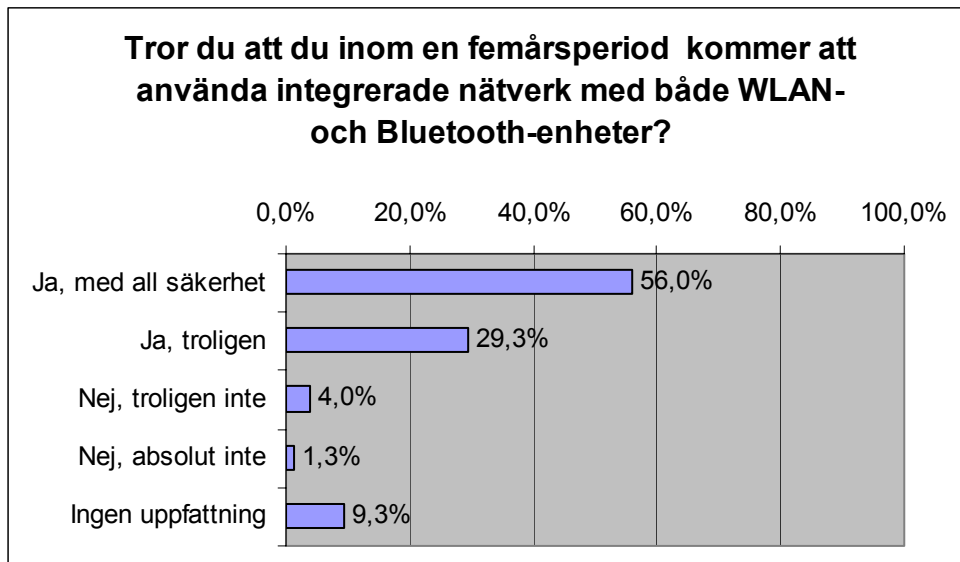
Figur 14. Fråga 2. Egen figur.

När det gäller var tekniken används var det två svarsalternativ som dominerade. 40,0 procent (30 stycken) använde tekniken på sin arbetsplats, medan 30,7 procent (23 stycken) använde tekniken hemma. De övriga svarsalternativen rangordnades som följer; Distansuppkoppling mot annat företag eller Internet 8,0 procent (6 stycken), På resan 6,7 procent (5 stycken), Annat (till exempel både hemma och på arbetsplatsen) 5,3 procent (4 stycken), Distansuppkoppling mot egna företaget 4,0 procent (3 stycken), Hos kund, mot kundens lokala nätverk 4,0 procent (3 stycken) och slutligen på offentliga platser 1,3 procent (1 stycken).



Figur 15. Fråga 3. Egen figur.

Majoriteten av respondenterna 56,0 procent (42 stycken) trodde att de med all säkerhet i framtiden skulle använda sig av integrerade nätverk med både WLAN och Bluetooth. 29,3 procent (22 stycken) trodde att de troligen skulle använda sig av integrerade nätverk i framtiden. 4,0 procent (3 stycken) antog att de troligen inte skulle använda sig av denna teknik i framtiden och 1,3 procent (1 stycken) trodde att de absolut inte skulle använda sig av integrerade nätverk i framtiden. 9,3 procent (7 stycken) hade i dagsläget ingen uppfattning i denna fråga.



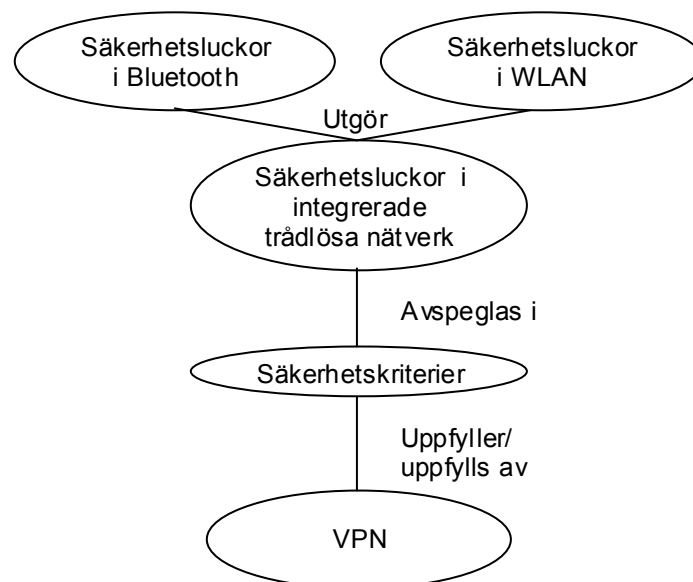
Figur 16. Fråga 4. Egen figur.

7 ANALYS

Vi har delat upp analysen i två delar som behandlar varsin del av syftet.

7.1 Kan VPN täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk?

I denna första del av analysen beskriver vi varför de båda teknikerna ska integreras. Därefter jämför vi säkerhetsluckorna i Bluetooth- och WLAN-nät var för sig. Ur jämförelsen får vi de säkerhetsluckor som kommer att finnas i integrerade trådlösa nätverk. Detta gör att vi kan formulera säkerhetskriterier som måste uppfyllas för att göra ett integrerat trådlöst nätverk säkert. Säkerhetskriterierna ställs sedan mot VPN. På detta vis kan vi avgöra om VPN innehåller funktioner som uppfyller dessa säkerhetskriterier och därmed gör VPN till en möjlig säkerhetslösning för integrerade trådlösa nätverk.



Figur 17. Graföver analys, del 1. Egen figur.

7.1.1 Integrerade trådlösa nätverk

Eftersom teknikerna Bluetooth och WLAN har olika styrkor och svagheter så kompletterar de snarare varandra än att konkurrera ut varandra. Detta gör att det finns många fördelar med att integrera teknikerna.

Bluetooth är ett billigt och effektivt sätt att få tillgång till ett trådlöst nätverk. Bluetooth är en radioteknik för korta avstånd. I sig är det inget revolutionerande, men det finns ett antal faktorer som gör den speciell. Den är billig, stabil, strömsnål och framför allt utnyttjar tekniken ett licensfritt frekvensband. Detta frekvensband utnyttjas även av WLAN, vars stora fördelar är hög dataöverföringskapacitet, stor räckvidd och kompatibilitet med övriga LAN-standarder. Både Bluetooth och WLAN använder sändningstekniken Spread spectrum, vilket gör att de klarar brusiga radioförhållanden.

Teknikerna har, som nämnts, sina respektive för- och nackdelar och ska användas där de kommer bäst till sin rätt. Ingen är enskilt överlägsen den andra. Bluetooth är billigare och mer strömsnålt än WLAN. Det är viktiga faktorer när det gäller massspridning och hur väl de ska fungera i bärbara batteridrivna enheter som handdatorer, laptops och mobiltelefoner. Å andra sidan har WLAN högre datakapacitet än Bluetooth, men kommer sannolikt inte vara lika väl spritt som Bluetooth, som snart kommer att finnas inbyggt i många produkter.

WLAN finns i dagsläget implementerat på företag och i Hotspots på offentliga platser. Bluetooth finns inbyggt i vissa typer av bärbara enheter och kommer att bli ännu mer utbrett i framtiden. Eftersom access pointen PX20 som är utvecklad av Possio är liten och trådlös är denna enkel att placera i befintliga Hotspots. Därmed kan ett integrerat trådlöst nätverk skapas och på så vis kan de båda teknikerna användas på det sätt de är bäst lämpade för. Fördelen är att en användare kan välja teknik efter sina förutsättningar, som mobilitet, utan för den skull vara begränsad till att enbart använda denna teknik. Till exempel kan en säljare på fältet med sin Bluetooth-telefon få tillgång till företagets LAN via en access point kopplad till ett WLAN.

7.1.2 Säkerhetsaspekter

Då både WLAN och Bluetooth är trådlösa och bygger på radioteknik är det enklare att avlyssna signalen än i ett fysiskt nätverk. Det är dock lättare att avlyssna signalerna från ett WLAN än från ett Bluetooth-nät då WLAN har betydligt större räckvidd. Denna säkerhetsrisk förebyggs dock delvis i själva grundtekniken genom att sändningstekniker (DSSS och FHSS) används, vilka ska vara svåra att avlyssna.

En annan gemensam risk är att en obehörig kan ta sig in i nätverket och blockera övrig trafik – denial-of-service.

I denna uppsats har vi fokuserat på intrång och avlyssning, detta är egentligen två aspekter av ett problem. Problemet är att skydda data från obehöriga och det finns olika säkerhetsåtgärder för detta. En säkerhetsåtgärd är att göra så att en inkräktare överhuvudtaget inte kan komma åt datatrafiken. Detta skyddar alltså mot intrång i nätverket. En annan säkerhetsåtgärd är att kryptera data så att den blir oläslig för en obehörig, vilket är ett skydd mot avlyssning. Dessa två åtgärder ger var för sig ett fullgott skydd för dataöverföring. Det säkraste alternativet är dock att använda båda typerna av skydd för att dessa ska kunna komplettera varandra. Även denial-of-service-attacker kan förhindras genom att skydda nätverket mot obehörig åtkomst.

De risker som föreligger för Bluetooth och WLAN kan således sammanfattas i två punkter. Risk för att en inkräktare tar sig in i nätverket och risk för att denne förstår informationen som sänds. En säkerhetslösning för integrerade trådlösa nätverk bör därför uppfylla två säkerhetskriterier;

1. En obehörig ska inte kunna ta sig in i det trådlösa nätverket och avlyssna informationen.
2. Om obehörig ändå gör ett intrång i det trådlösa nätverket ska denne inte förstå vad som sägs.

Det finns säkerhetslösningar för Bluetooth-nät respektive WLAN som uppfyller dessa säkerhetskriterier, dessa är autentisering samt kryptering. Dessa lösningar är dock

teknikspecifika och för integrerade trådlösa nätverk krävs en heltäckande säkerhetslösning. Om de teknikspecifika säkerhetslösningarna för exempelvis kryptering används när data skickas från ett Bluetooth-nät till ett WLAN-nät måste datan dekrypteras och krypteras igen i access pointen. För ett kort ögonblick är datan okodad, vilket är en säkerhetsrisk.

VPN används för att skapa säkra uppkopplingar i osäkra medium, ofta Internet. VPN innebär att ett till synes privat nätverk skapas. Eftersom det underliggande mediet är osäkert så går det i ett VPN att avlyssna trafiken till skillnad från ett riktigt privat nätverk. VPN skyddar dock datan med hjälp av autentisering, tunnling, kryptering och i vissa fall brandväggar. Då både Bluetooth och WLAN kan använda IP-protokollet är det tekniskt möjligt använda IP-baserade VPN-lösningar på dessa nätverkstekniker.

7.1.2.1 Kriterium 1 – neka obehörig åtkomst till nätverket

I en VPN-lösning används autentisering för att hindra obehöriga för att ta sig in i nätverket. I WLAN är det nätverkskortets MAC-adress som autentiseras. MAC-adressen är knuten till nätverkskortet och det är därför egentligen nätverkskortet som ges behörighet. Till skillnad från autentiseringsprocessen som används i WLAN så är det användarens identitet och inte hårdvarans identitet som avgör om användaren har tillträde till nätverket eller inte då VPN används. Med en VPN-lösning är alltså inte stöld av hårdvara något hot, förutsatt att inte användarens identitet, till exempel lösenord eller certifikat, finns lagrade i hårdvaran.

Vissa VPN-lösningar använder sig av en ömsesidig autentiseringsprocess, det vill säga att servern kontrollerar klientens/användarens identitet samt att klienten även kontrollerar serverns identitet. Detta för att undvika att obehörig får åtkomst till nätverket genom att utge sig för att vara någon annan, så kallad spoofing.

En del VPN-lösningar tillämpar även brandväggar för att ytterligare skydda sig mot inkräktare genom att begränsa trafiken.

7.1.2.2 Kriterium 2 – göra data oläslig för obehörig

Det vanligaste sättet att göra informationen oläslig för en inkräktare är att kryptera data. VPN kan använda symmetrisk eller asymmetrisk kryptering. Kryptering ingår även i WLAN- och Bluetooth-standarderna. I dessa standarder är det symmetriska krypteringsalgoritmer som används, men teknikerna använder inte samma algoritm.

I och med att symmetrisk kryptering anses vara relativt säker och inte kräver så mycket CPU-kraft passar den i trådlösa nätverk. Detta gäller främst för små enheter som mobiltelefoner och handdatorer, där processorn av utrymmes- och energiskäl inte är så kraftfull. En VPN-lösning som använder symmetrisk kryptering kan till skillnad från krypteringsteknikerna för WLAN och Bluetooth användas i hela det integrerade trådlösa nätverket. På detta vis skulle data alltså kunna krypteras med en sorts krypteringsalgoritm ända från handdatorn med ett Bluetooth-kort över en access point vidare över ett WLAN och ända fram till slutdestinationen.

Data som sänds i en VPN-tunnel är krypterad, men själva tunnlingen skyddar också data mot insyn från omvärlden. Med en VPN-tunnel är det möjligt att skapa en point-to-point-förbindelse i integrerade trådlösa nätverk för att säkra överföringen av data. Detta görs genom att datapaketet kapslas in så att paketet kan färdas över vilken typ av nätverk som helst oavsett vad sändaren använder för protokoll. Detta gör att datan är krypterad hela vägen från

sändare till mottagare och dekrypteras inte någonstans på vägen. Att skapa en point-to-point-förbindelse på detta vis är inte möjligt idag med någon annan existerande teknik.

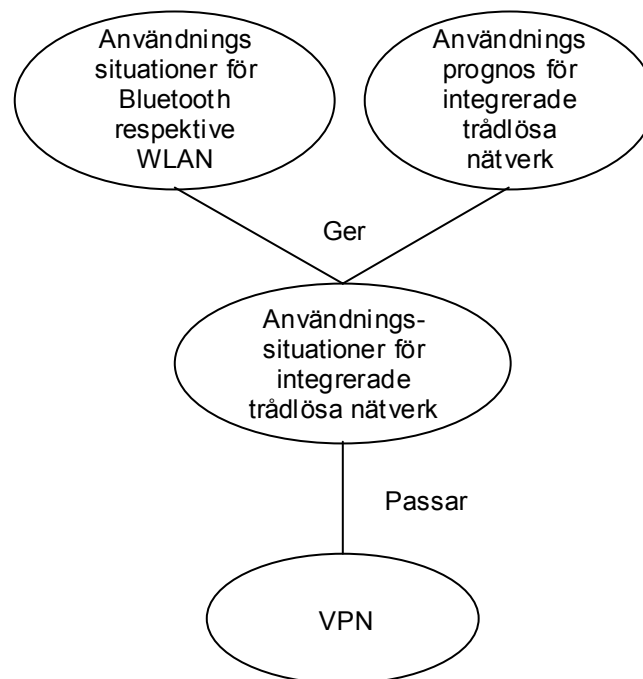
7.1.2.3 Tunnling – Kriterium 1 och 2

Tunnlingen medför att det en avlyssnare fångar upp av datatrafiken säger väldigt lite av det som sänds och det är inte endast en krypteringsalgoritm som ska knäckas för att innehållet ska friläggas. Tunnlingen är det virtuella privata nätverkets motsvarighet till det privata nätverkets kabel. Funktionen med tunnling liknar till viss del sändningsteknikerna DSSSs och FHSSs funktioner, nämligen att det trots det osäkra mediet ska vara svårt att avlyssna datatrafiken.

Tunnlingsprocessen uppfyller båda de kriterier för säkerhet som vi har ställt upp. En tunnel kan endast upprättas mellan autentiserade användare (kriterium 1) och informationen i tunneln är oläslig för obehöriga (kriterium 2).

7.2 Hur passar olika VPN-lösningar i de vanligaste användningssituationerna för integrerade trådlösa nätverk?

I den andra delen av analysen tittar vi på vilka användningssituationer som visat sig vara vanligast för Bluetooth respektive WLAN. Om användarna till dessa tekniker är positiva till att använda integrerade trådlösa nätverk i framtiden så torde samma användningssituationer dominera i dessa nätverk. Eftersom detta var fallet har vi analyserat hur väl olika VPN-lösningar passar i dessa situationer, både tekniskt och praktiskt. Vi tittar till exempel på vad som kan påverkas av mobilitet, utrymme och kapacitet.



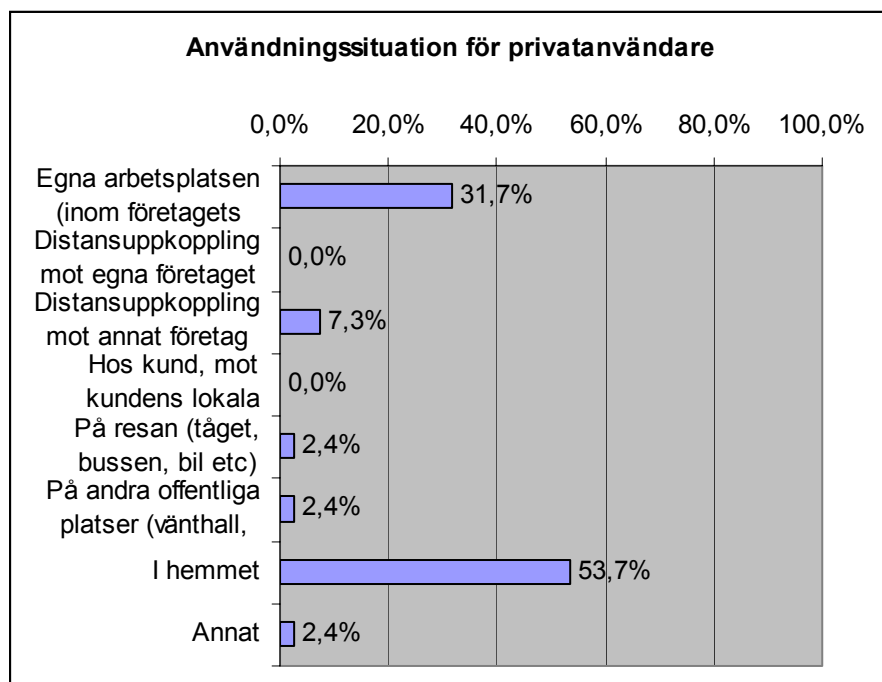
Figur 18. Graföver analys, del 2. Egen figur.

Enligt enkätundersökningen är det betydligt fler som använder WLAN (66,7 procent) än Bluetooth (22,7 procent), en liten grupp använder båda teknikerna (10,7 procent). Enligt Forresters prognoser kommer dock Bluetooth att implementeras i betydligt fler produkter inom de närmsta åren, vilket kan förändra användningsfördelningen. Sammanlagt var 85,3 procent av respondenterna positiva till att använda integrerade trådlösa nätverk inom en

femårsperiod. Detta kan ses som indikation på att användningssituationerna för integrerade trådlösa nätverk kommer att vara desamma som för de separata nätverken.

7.2.1 Användningssituationer för privat användare

Mer än hälften av respondenterna använde de trådlösa teknikerna privat (54,7 procent). Majoriteten av dessa använder tekniken i hemmet (53,7 procent). Den näst största gruppen (31,7 procent) använde tekniken på den egna arbetsplatsen i privat syfte.



Figur 19. Användningssituationer för privat användare. Egen figur.

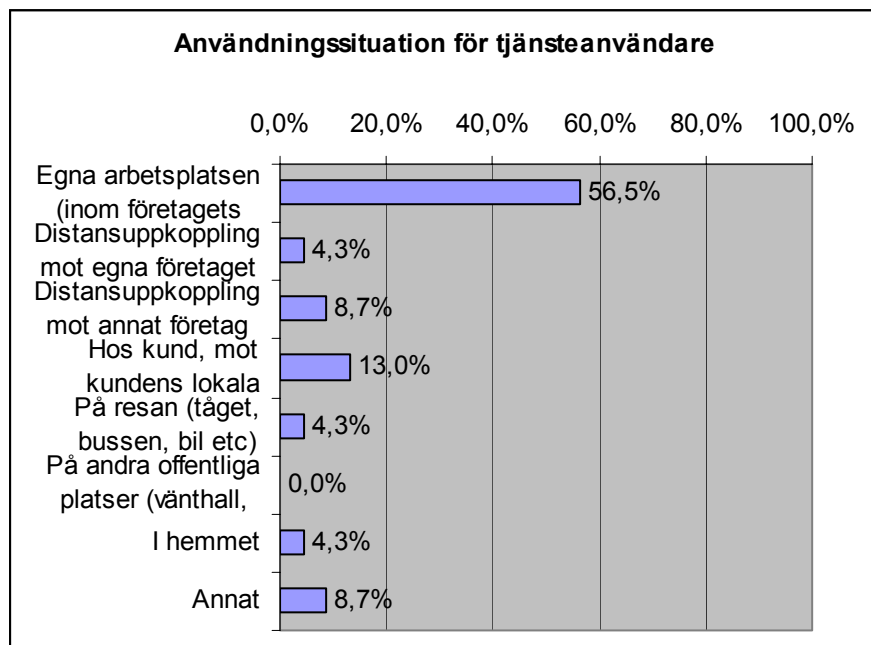
Situationen är alltså som följer: de flesta användarna av Bluetooth- eller WLAN-teknik använder denna teknik privat i det egna hemmet. En relativ stor del av privat användarna använder dock tekniken på den egna arbetsplatsen.

Den typ av VPN som används i privat syfte i hemmet är Remote Access då användaren kopplar upp sig mot Internet.

Vad gäller autentisering finns det ett antal metoder att välja mellan. Dessa passar mer eller mindre bra i olika situationer. I hemmet är säkerhetskraven oftast inte så stora om uppkopplingen ska användas i privat syfte, till exempel surfa på Internet. Vad gäller bankärenden och andra tjänster med högre säkerhetskrav ligger ansvaret för säkerheten hos den som erbjuder tjänsten och inte hos användaren. Autentiseringsmetoden behöver med andra ord inte vara av det säkraste slaget. Biometrisk autentisering skulle till exempel vara onödigt resurskrävande och komplicerat. Beroende på hur hög säkerhet användaren vill ha skulle det vara lämpligt med ett enkelt lösenord, engångslösenord eller liknande. I denna situation passar ett lösenord eller ett certifikat med eller utan smartcard. Om användaren delar datorn med andra i hemmet som inte ska tillgång till VPN-lösningen är det mer lämpligt med ett lösenord än till exempel ett certifikat som är lagrat på hårdvaran i en oskyddad fil.

7.2.2 Användningssituationer för tjänsteanvändare

Majoriteten av tjänsteanvändarna använder tekniken på arbetsplatsen (56,5 procent). Övriga tjänsteanvändare är relativt jämnt fördelade mellan resterande användningssituationer.



Figur 20. Användningssituationer för tjänsteanvändare. Egen figur.

Tjänsteanvändaren kan använda sig av alla tre VPN-typer; Remote Access mot Internet eller annat företag, Intranetbaserat inom den egna arbetsplatsen eller Extranetbaserat om det egna företagets LAN är sammankopplat med något annat företags LAN.

På ett företag är behöriga användare kända och kan finnas i anställningsregister eller liknande. Detta får till följd att valfriheten är relativt stor vad gäller autentiseringssätt. Det är teoretiskt sätt inga större problem att samla in samtliga anställdas fingeravtryck. Ett företag har även mer resurser, vilket gör att mer kostsamma metoder kan användas om säkerheten kräver det. Detta gäller oavsett om användaren använder uppkopplingen i tjänsten eller privat. Att användarna är kända och lättillgängliga på ett företag gör att distributionen av privata nycklar för symmetrisk kryptering inte är något problem.

Då användaren kopplar upp sig mot nätverk från ett företag är det viktigt med hög säkerhet eftersom användaren då befinner sig innanför företagets brandvägg. Brandväggen kan därför inte skydda företagets lokala nätverk. Därför kan det vara mindre lämpligt med enkla lösenord eller certifikat lagrade på användarens hårddisk.

7.2.3 Icke-mobil/Stationär användning

Hemmet och arbetsplatsen är två platser som är relativt oföränderliga vad gäller uppkoppling. Användaren befinner sig inom ett begränsat område, inom byggnadens fyra väggar. I och med den begränsade mobiliteten har det inte så stor betydelse för företags- eller hemanvändaren om VPN-lösningen är hård- eller mjukvarubaserad. För en hemanvändare kan det däremot vara en stor investering att införskaffa en server. Det är dessutom utrymmeskrävande.

När det gäller kryptering finns det också aspekter som har med användningssituationen att göra. För användaren är det enklare att använda asymmetrisk kryptering, då användarens krypteringsnyckel är publik och således inte behöver distribueras till varje specifik användare. Denna form av kryptering kräver dock mer CPU-kapacitet, vilket kan vara till nackdel i en trådlös enhet då CPU-kapaciteten ofta begränsas av storlekskrav. Eftersom det är så att trådlösa nätverk används främst i hemmet eller på arbetsplatsen så skulle det kunna vara så att användarna främst använder en PC. I sådana fall är CPU-kapaciteten större och val av krypteringsalgoritm behöver därför inte avgöras av detta. Om det däremot är så att användarna använder små bärbara enheter på sin arbetsplats och i hemmet så kan CPU-kapaciteten vara av stor betydelse.

7.2.4 Mobil användning

Vad gäller de användningssituationer där användaren är mer mobil, med andra ord ute på fältet och rör sig ser förutsättningarna något annorlunda ut. De flesta VPN-lösningar är främst utvecklade för fysiska nätverk, även om de fungerar i trådlösa nätverk. Det finns dock tekniska aspekter som är specifika för trådlösa nätverk. Dessa tekniska aspekter kan ställa till problem i vissa användningssituationer. Exempel på dessa problem är dålig stabilitet i uppkopplingen samt oberäknelig tillgång till nätverket. Dessa problem kan lösas genom ytterligare mjukvara till den traditionella VPN-lösningen eller att använda en VPN-lösning som är speciellt anpassad för trådlösa nätverk. Färdas användaren exempelvis från flygplatsen till kontoret ska uppkopplingen kännas stabil och kontinuerlig oavsett kopplas upp mot olika Hotspots under resans gång. Det är detta som kallas för sömlös roaming.

8 SLUTSATSER

Kan VPN täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk?

För att kunna bedöma om VPN kan täcka de säkerhetsluckor som finns i integrerade trådlösa nätverk har vi ställt upp två säkerhetskriterier som måste uppfyllas. Säkerhetskriterierna är:

1. En obehörig ska inte kunna ta sig in i det trådlösa nätverket och avlyssna informationen.
2. Om obehörig ändå gör ett intrång i det trådlösa nätverket ska denne inte förstå vad som sägs.

VPN innehåller funktioner för att hindra att obehöriga kan ta sig in i det virtuella privata nätverket. Exempel på detta är autentisering samt brandväggar, med vilka en användares behörighet kan kontrolleras innan denna ges tillträde till nätverket.

Om någon obehörig ändå skulle lyckas ta sig in i nätverket använder VPN kryptering som gör data oläslig för inkräktaren.

Den funktion i VPN som kallas tunnling uppfyller de båda säkerhetskriterierna. Det kan endast upprättas en tunnel mellan autentiserade användare (kriterium 1). Vidare är informationen som sänds i tunneln oläslig för en inkräktare (kriterium 2).

VPN har funktioner som uppfyller både kriterium 1 och 2. Således har VPN alla förutsättningar för att lösa de säkerhetsluckor som finns i integrerade trådlösa nätverk.

Hur passar olika VPN-lösningar i de vanligaste användningssituationerna för integrerade trådlösa nätverk?

Privatanvändare i hemmet

Befinner sig användaren i hemmet och använder det integrerade trådlösa nätverket i privat syfte är säkerhetskraven i allmänhet inte lika höga som på arbetsplatsen. Det är därför onödigt resurskrävande att använda sig av biometriska metoder för autentisering. I denna situation passar ett lösenord eller ett certifikat med eller utan smartcard. I hemmet är det lämpligt med en mjukvarubaserad VPN-lösning då en hårdvarubaserad lösning dels tar plats och dels är en stor investering för en privatperson. För privatanvändare är det mest praktiskt att använda asymmetrisk kryptering beroende på att nyckelhanteringen är mindre komplicerad. Detta förutsatt att hårdvaran har tillräcklig kapacitet för detta.

Privat- och tjänsteanvändare på det egna företaget

På ett företag finns det större valfrihet vad gäller autentiseringssätt eftersom användarna är kända. Smartcards och lösenord kan delas ut eller uppgifter om fingeravtryck lagras. Däremot är det viktigt med en hög säkerhet på företaget då användaren befinner sig innanför företagets brandvägg. Därför kan det vara mindre lämpligt med enkla lösenord eller certifikat lagrade på användarens hårddisk. På företaget passar symmetrisk kryptering eftersom distributionen av

privata krypteringsnycklar inte är något problem. Att använda symmetrisk kryptering ger även större valfrihet vad gäller hårdvara.

Icke-mobil/Stationär användning

Teknikerna som ingår i integrerade trådlösa nätverk (WLAN och Bluetooth) används främst i privat syfte i hemmet eller på det egna företaget. På dessa platser är det inte av så stor betydelse om VPN-lösningen är hårdvaru- eller mjukvarubaserad eftersom företaget inte är mobilt, det är fysiskt förankrat i sina lokaler.

I de vanligaste användningssituationerna finns det således inget hinder för att implementera en VPN-lösning då det finns varianter som passar de olika situationerna.

9 DISKUSSION

När vi påbörjade denna uppsats förväntade vi oss att teknikerna Bluetooth och WLAN i största utsträckning användes i mobila sammanhang, såsom på caféet, flygplatsen eller i taxin. Det visade sig dock att teknikerna mest användes i hemmet eller på det egna företaget. Vid närmare eftertanke är detta inte så uppseendeväckande då det trots allt är på dessa platser de flesta människor tillbringar största delen av sin tid. Denna upptäckt innebär att situationerna inte är så olika de situationer där VPN i dagsläget används.

I denna uppsats har vi kommit fram till att en VPN-lösning kan användas i integrerade trådlösa nätverk. Ett företag som vill implementera en VPN-lösning kan välja mellan varianter utifrån vår analys beroende på användningssituation.

I vidare forskning är det lämpligt att undersöka hur säkra VPN-lösningarna egentligen är, till exempel hur lätt en krypteringsalgoritm kan knäckas.

En annan infallsvinkel i fortsatta studier på området är var VPN-klient respektive VPN-servern skall placeras i förhållande till befintliga brandväggar. Brandväggen kan eventuellt förlora sin funktion beroende på var VPN-klienten placeras. Vilken placering som är lämplig varierar troligtvis mellan olika användningssituationer.

För att få en bild över den totala säkerhetsproblematiken i integrerade trådlösa nätverk bör förutom avlyssning och intrång även störning beaktas. Vi ser dock störning som ett helt eget problemområde, lika viktigt men mycket olika avlyssning och intrång både vad gäller effekt och åtgärder. Vid störning får en sabotör exempelvis inte tillgång till informationen.

Vi hade kunnat komplettera denna uppsats med att utföra experiment för att testa VPN i integrerade trådlösa nätverk praktiskt. I denna uppsats har vi teoretiskt fastställt att de tekniska förutsättningarna existerar. Ett argument för att utföra experiment är att vi verifierar våra källors riktighet. Vi har använt oss av ett flertal källor, både i bok- och i elektronisk form. Dessa källor motsäger inte varandra, vilket gör dem mer trovärdiga. Visserligen skulle samstämmigheten bero på att alla källor bygger på en gemensam informationskälla. Denna risk tror vi kan vara relativt stor när det gäller artiklar. Den borde vara mindre vad gäller andra Internet-källor, såsom White Papers, och förhoppningsvis minimal när det kommer till tryckt litteratur. Vi har nått informationen på olika sätt och de olika källorna har ingen synlig anknytning till varandra.

Den fakta vi har varit intresserad av i denna uppsats innehåller inga känsliga uppgifter som någon skulle ha intresse av att förvanska. Det är inte heller fråga om fakta där värderingar spelar in. Därför torde en annan uppsättning källor ge samma resultat.

Det skulle även vara intressant att skriva en liknande uppsats om ett år, då delen om integrerade trådlösa nätverk kan baseras på den aktuella användningssituationen istället för som nu på uppskattningar om framtida användningssituationer.

KÄLLFÖRTECKNING

Skriftliga källor

Litteratur

Bray, Jennifer & Sturman Charles F., *Bluetooth – connect without cables*, Prentice Hall Inc, Upper Saddle River, 2001

Englander, Irv, *The Architecture Of Computer Hardware And Systems Software – An Information Technology Approach*, Wiley & Sons, USA, 1996

Ewert, Magnus, *Datakommunikation – Nu och I framtiden*, Studentlitteratur, Lund, 1999

Garfinkel, Simson, *PGP Pretty Good Privacy*, Reilly & Associates Inc., Sebastopol CA, 1995

Geier, Jim, *Wireless LANs – Implementing High Performance IEEE 802.11 Networks*, SAMS, Indiana, USA, 2002

Jensen, Stig, Gjelstrup, Arne och Berti, Valentino, *Datakommunikation*, Liber, Stockholm, 2000

Kosiur, Dave, *Building and Managing Virtual Private Networks*, John Wiley & Sons, 1998

Miller, Brent A., *Bluetooth revealed*, Prentice Hall Inc, Upper Saddle River, 2001

Miller, Michael, *Discovering Bluetooth*, Sybex, Alameda, 2001

Muller, Nathan J, *Bluetooth demystified*, McGraw-Hill, New York, 2001

Shea, Richard, *L2PT – Implementation and operation*, Addison-Wesley, Massachusetts, 2000

Singh, Simon, *Kodboken*, Norstedts förlag, Stockholm, 1999

Kompendium

Ottosson, Benny, *Internet & TCP/IP*, ESA, Högskolan i Örebro, 1995

Tidningsartiklar

Andersson, Niklas, *Ta tunneln över till den säkra sidan*, Säkerhet och sekretess, nr 4, 2001

Bodin, Patrik, *Säker överföring tack vare IPSec*, Nätverk och Kommunikation, nr 18, 2001

Lindqvist, Jonas, *Bättre e-handel med hjälp av PKI*, Nätverk och Kommunikation, nr 18, 2001

Ogelid, Håkan, *700 000 fler trådlösa användare i månaden*, Computer Sweden, nr 111, 2001

Ricknäs, Mikael, *Trådlöst dominerar på Comdexmässan*, Computer Sweden, nr 118, 2001

Ricknäs, Mikael, *Virtuella privata nät skyddar trafiken över öppet nät*, Computer Sweden, 2001-11-02

Rittsel, Per, *Trådlösa lan i pc:n, Bluetooth i resten*, Computer Sweden, nr 113, 2001

White Papers

AppGate, *AppGate White Paper – Version 4*, 2001-06-18

Columbitech, *Extending VPN Technology for Wireless Access*, 2001

Microsoft, *Virtual Private Networking: an overview – White Paper*, 1999

Trudeau Pierre, *Building Secure Wireless Local Area Networks – a White Paper by Colubris Networks Inc.*, 2001

Wavelink, *Wireless Network Security – White Paper*, 2001-10-10

Källor från Internet

Arbaugh William A, Shankar Narendar, Wan Y.C. Justin, *Your 802.11 Wireless Network has No Clothes*, Department of Computer Science, University of Maryland, 2001-03-30
<http://www.cs.umd.edu/~waa/wireless.pdf>, 2001-10-20

Columbitech Wireless VPN™ - Wireless Independence Within A Strong Security Framework, Columbitech
www.columbitech.se/documents/columbitechWVPNProductSheet.pdf, 2001-11-20

En produktberoende introduktion, Communica Datadistribution AB, 2001-06-05
<http://www.communica.se/bluetooth/introduktion.htm>, 2001-10-08

Gilb, James, *TX power for LCW*, Mobilian,
<http://grouper.ieee.org/groups/802/15/arc/802-15-3list/msg00006.html>, 2001-12-12

Introduction To Cryptography, User's Guide PGP 7.0

<http://www.pgpi.org/doc/guide/7.0/en/intro/>, 2001-11-16

Kumria, Anand, *An Introduction to PGP*, University of Technology, Sidney, 1997-05-12

<http://www.progsoc.uts.edu.au/~wildfire/pgp/pgp.html#Cryptography>, 2001-12-13

Lawton, George, *Lock up your Wireless LAN*, CNET Enterprise

<http://enterprise.cnet.com/enterprise/0-9567-7-6803660.html>, 2001-11-22

Matthews, Brian D., m fl, *Standards Based Wireless Networking With Linux*, The linux-wlan Company

<http://www.linux-wlan.com/writings/std-wlan-whitepaper.html>, 2001-10-16

McDaid, Cathal, *Bluetooth Security - Evaluation & Conclusion*, Palowireless Bluetooth Research Center, 2001-03

http://www.palowireless.com/bluearticles/cc2_security3.asp, 2001-10-24

Nationalencyklopedien

<http://www.ne.se>, 2002-01-05

OpenBSD får stöd i maskinvara för IPsec-kryptering, OpenBSD

<http://www.openbsd.org/reprints/openbsd-hwcrypto.html>, 2002-01-02

PCTechGuide, *Wireless networks*

http://www.pctechguide.com/29net2.htm#Wireless_networks, 2001-10-16

Possio

<http://www.possio.com/spread.asp?dynfile=px20intro&cat=2&loop=2&dh=2>, 2001-11-21

Savage, Clive, European PR Manager, *Wireless LAN And Bluetooth Will Coexist In Europe*, pressrelease, Forrester Research B.V., 2001-10-22

<http://www.forrester.com/ER/Press/Release/0,1769,642,00.html>, 2001-11-26

Tyson, Jeff, *How Virtual Private Networks Work*, HowStuffWorks

www.howstuffworks.com/vpn.htm/printable, 2001-11-13

Wireless LAN Security - The Growth of Wireless LANs, Cisco Systems, 2001-04-11

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm, 2001-10-10

WLANA, The Wireless LAN Association

http://www.wlana.com/learning_center.html, 2001-10-10

E-post

Johansson, Pelle, 2001-12-04

Muntliga källor

Mårild, Kristoffer, Software Developer, Possio

Quast, Detlef, Universitetslektor, Örebro Universitet

Sundman, Mikael, Senior Technical Manager, Possio

Söderberg, Ulf, Vice President R & D, Possio

Thoresson, Agneta, Service, AppGate