Trådlösa nätverk i Linköping
Ett projekt inom kursen TDDC03
vid Linköpings universitet

Claes Ahrén
Camilla Jansson
Magnus Wiktor

Sammanfattning

Denna rapport redovisar resultatet av ett projekt inom kursen TDDC03 Information Security vid Linköpings universitet. Innehållet i denna rapport och mer därtill finns tillgängligt på http://wlan.no-ip.org. Projektet har innefattat:

- *Konfigurera en dator för att logga trådlös nätverkstrafik.*
- *Logga trådlösnätverkstrafik runt om i Linköping.*
- *Analysera resultatet av detta.*

1. Syfte och målgrupp

Det huvudsakliga syftet med denna rapport är att presentera ett tillvägagångssätt så att läsaren får en enkel guide till hur man kan genomföra en enkel avlyssning av trådlösa nätverk. Anledningen till detta huvudsyfte är att det tog oss själva mycket tid till att få utrustningen rätt konfigurerad och att vi saknade en bra guide. Målgruppen är därför främst sådana som oss själva det vill säga studenter inom datavetenskapliga ämnen med ingen eller lite erfarenhet av Linux.

2. Kartläggning

Vi har valt att framför allt kartlägga centrum av Linköping så komplett som möjligt. Detta har inneburit att vi har kört på i princip alla gator som gick i centrum. För att kunna jämföra detta med något har vi också valt att köra i Mjärdevi. Vi har sedan jämfört centrum med Mjärdevi. Frågeställningen är om den stora andelen teknikföretag i Mjärdevi är mer säkerhetsmedvetna än de företag som har trådlöst nätverk i centrum. Vi antog att det borde vara så.

2.1. Vad är intressant att titta på?

Ur det perspektivet vi har valt har det varit intressant att undersöka följande saker:

- Vi vill veta hur många som använder WEP. Totalt, i stan och i Mjärdevi. Anledningen till detta är att ett nätverk med WEP påslaget är ett svårare byte än ett nätverk som inte har slagit på WEP. Vi är intresserade av hur många som antingen väljer att vara ett lätt byte eller som kanske inte är medvetna om att de är det.
- Vi vill också veta om nätverken använder sig av default SSID eller om de bytt SSID. En lista med default SSID finns här: http://www.wardriverz.com/access_point.htm. Den hjälpte oss att se om SSID var bytt eller inte i vissa fall där vi var osäkra.
- Ser vi något samband mellan att default SSID finns kvar och att WEP inte är påslaget? Det vore rimligt eftersom accesspunkter levereras på det sättet. Den som inte har bytt SSID har förmodligen inte slagit på WEP heller.
- Var det några som broadcastade "No SSID". Hade de WEP påslaget eller avslaget?

3. Juridiska aspekter

Vän av ordning kan tycka att avlyssning av trådlösa nätverk är olagligt men så är inte fallet i Sverige. En grundläggande regel för lagar på området är att etern är fri att lyssna på så mycket man vill. Det finns heller inga lagar som gör det straffbart att knäcka krypteringar på den trafik man lyssnar av trådlöst. Vad som dock kan vara straffbart är att skicka information trådlöst som kan lyssnas av. Till exempel kan ett sjukhus som installerar ett trådlöst nätverk göra sig skyldigt till brott mot sekretesslagen om det går att lyssna av trafiken, dekryptera den och plocka fram patientinformation. (En mer utförlig genomgång på området kan läsas i *Laglöst land,* ComputerSweden nr 33 2003.)

4. Utrustning

Följande utrustning användes för detta projekt:

- Dator: Dell Latitude CPi D266XT
- Nätverkskort: Netgear MA401, 802.11b trådlöst nätverkskort
- Accesspunkt: Netgear ME102, 802.11b trådlös accesspunkt
- GPS: GM48 RS 232/PS 2
- Mjukvara: Linux, Kismet, GPSDrive, GPSD, gpsmap

5. Systemets delar

Debian (unstable): Linux OS
Kismet: Hittar och identifierar trådlösa nätverk. Ger möjlighet till GPS support via GPSD (se nedan). Kismet loggar nätverken och dess position och ger möjlighet till att generera grafiska kartor över nätverkens geografiska läge.
GPSD: GPS-mottagaren sänder NMEA; en seriell dataström. Gpsd är en daemon som parsar NMEA och översätter positionsdata till enklare format.
GPSDrive: Mjukvara för GPS navigation. Versioner senare än 1.17 innehåller gpsd.

När Kismet upptäcker en trådlös accesspunkt, lagras information om nätverket och dess position i en SQL-databas. En ikon (ett hänglås som är låst eller olåst beroende på om WEP används) visas i realtid på navigationskartan i GPSDrive.

6. Konfiguration

För att få systemet att fungera krävdes att vi kompilerade en egenkonfigurerad linuxkärna. Detta samt de andra delarna i systemet beskrivs här.

6.1. Allmänt

Genom att använda apt-get kan man hämta hem och installera mjukvara. Detta är mycket användbart när man får kompileringsfel som beror på att efterfrågad funktionalitet inte finns installerad i systemet (vilket inträffar allt som oftast).

På http://www.debian.org/distrib/packages finns möjlighet att söka efter debian-paket, som man kan installera med apt-get.

6.2. Ladda ner källkoden för kärna 2.4.20

Kan hämtas här:
http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.20.tar.bz2.

6.3. Drivrutin för nätverkskortet

Kärnans drivrutin för nätverkskortet måste uppdateras för att kunna köras med Kismet. Uppdateringen går att hämta på följande webbadress: http://airsnort.shmoo.com/orinocoinfo.html. Vi valde version 3.2.1. Lagra den i ../linux/drivers/net/wireless (linux är katalogen där vi lagt kärnan). Patchen appliceras genom att göra följande i ../linux/drivers/net/wireless

```
pcmcia-cs-3.2.1-orinoco-patch.diff | patch -p1
```

6.4. Konfiguration av kärnan

Det finns flera olika möjligheter att konfigurera kärnan på. Vi använde främst make menuconfig, som öppnar ett enkelt GUI där man kan uppdatera olika funktioner. Konfigurationen sparas i filen .config (filen kan laddas ner från hemsidan).

Här finns en allmän guide för hur man kompilerar en linux-kärna:
http://www.linux.org/docs/ldp/howto/Kernel-HOWTO.html

6.5. Ethereal

Vi installerade ethereal 0.9.8. Troligtvis behövs inte ethereal för Kismet, vi gjorde detta som en ren försiktighetsåtgärd.

6.6. ImageMagick

Gpsmap, som finns i Kismet, använder Kismets .gps-filer för att generera kartor över nätverkens positioner. ImageMagick används av gpsmap och måste eventuellt installeras. Vi använde version >= 5.5.2 och installerade med apt-get.

6.7. GPSDrive

Installationen av GPSDrive görs smidigast genom apt-get eftersom det finns debian-paket för version 1.32

6.8. Kismet

Vi använde version 2.8.1, som finns att ladda ner på http://kismetwireless.net . Vi var även tvungna att ändra i koden för Kismet för att få GPS-mottagaren att fungera ihop med programmet, se nedan under "Kodändringar i Kismet för att kunna lagra GPS-positioner".
Den uppdaterade källkoden kompilerades genom;

```
./configure
make dep
make
```

6.9. Konfigurera Kismet

Ändra i filen kismet.conf, de viktigaste bitarna är;

```
servername=Kismet
suiduser=Ditt_Användarnamn
source=orinoco,eth0,Kismet
```

6.10. Start av systemet

Som *root* Sätt kortet i monitor mode och starta gpsd daemon.

```
kismet_monitor -H   (-H används för att hoppa mellan olika kanaler)
gpsd -p /dev/ttyS0  (ttyS0 är den port som GPS-mottagaren använder)
```

Som *Ditt_Användarnamn* Starta Kismet

```
kismet
```

Starta GPSDrive i något fönstersystem.

6.11. Kodändringar i Kismet för att kunna lagra GPS-positioner

För att få GPS-informationen att fungera tillsammans med Kismet kan några ändringar krävas i koden. Detta beror på vilken GPS som används. Vi har testat med en slags Garmin och då behövde koden inte ändras. Med den GPS vi använde krävs vissa ändringar i koden.

Om detta var något felaktigt i GPS:en eller inte vet vi inte, men den lyckades inte returnera en fix position trots att den hade fyra satelliter eller fler. (Fyra satelliter är det normala för att kunna bestämma en fix position). Enligt beskrivningen av GPS:en har den en 4-8 meters noggrannhet 95 % av tiden. Därför ändrade vi koden till att alltid ha en fix position oavsett vad NMEA-informationen säger.

Det som behöver ändras är där Kismet skannar och läser in GPS-information från gpsd. Kismet frågar gpsd kontinuerligt efter GPS-information. Gpsd läser in NMEA från GPS:en och ger ut informationen i ett annat, eget, format. Kismet frågar gpsd efter denna information hela tiden. Det är där vi ändrar koden och ignorerar fix position genom att sätta den till 2. Ändringen i koden för Kismet är gjord i funktionen "int GPSD::Scan()" i gpsd.cc. Där sätter vi mode=2 efter att information från gpsd-daemon lästs in.

7. Tillvägagångssätt

7.1. Arbetsgång

Den större delen av arbetet var att få datorn rätt konfigurerad med ett fungerande Linux med rätt drivrutiner för nätverkskortet, samt att installera alla program som behövdes och att få dessa att fungera korrekt.

Ett av problemen vi hade var med GPS:en. GPSD läste in data från GPS:en. Kismet anropade GPSD för att få informationen från GPS:en och använde denna data för att lagra filer med gps-positionen ihop med en funnen accesspunkt. Utan GPS-information kunde Kismet inte veta var en accesspunkt hade hittats. Problemet var att Kismet inte fick in en fix position. Detta behövdes för att kunna lagra en position. För att lösa detta krävdes både analys av GPSD:s output och källkoden för både GPSD och Kismet. Dessutom lånade vi en annan GPS, vilken klarade av att ge en fix position. Med hjälp av denna data kunde vi ändra i källkoden så Kismet alltid tog första bästa position då den hittade en accesspunkt. Detta medförde att positionerna inte alltid var helt exakta. Å andra sidan gick det nu att få ungefärliga positioner för de hittade nätverken och att därmed kunna generera kartor som resultat. Dessutom visades positioner i GPSDrive direkt när ett nytt nätverk hittades.

Då konfigurationen var utförd och utrustningen fungerade kunde nätverksavlyssningen påbörjas. Genomförandet av avlyssningen utfördes till större del med hjälp av motorfordon. Då nyttjande av motorfordon medför substantiella kostnader har endast begränsade områden avlyssnats. Vi fokuserade på centrum av Linköping samt företagsparken Mjärdevi. Vi har även viss data från bostadsområdet T1. Kismet gjorde då det mesta av jobbet. GPSdrive var till stor nytta under själva körningarna för att kunna se ”live” vad som upptäcktes. I efterhand användes sedan filer som Kismet sparade för att producera kartor och extrahera statistik om nätverken.

7.2. När allt fungerade

Vi ställde in nätverkskortet i monitormode. Då lyssnar den på all trafik som den kan hitta. Dessutom lät vi kortet lyssna på olika kanaler för att kunna hitta nätverk som använder alla möjliga frekvenser. Sedan startade vi GPSD för att få data från GPS:en. Vi startade även Kismet och GPSDrive i nämnd ordning. Därefter var det bara att börja leta nätverk. Vi kunde följa sökning direkt med hjälp av GPS-drive. Där kunde vi se var vi var, vart vi åkte och vilka nätverk vi hittat. Kismet lagrade dessutom flera olika filer om allt som t.ex. alla accesspunkter som hittats och rutten som vi åkt. Dessa använde vi efter körningen för att bl.a. generera kartorna.

Vi hade dock ett problem som uppstod då och då. Nätverkskortet låste sig och returnerade samma fel om och om igen. Ibland fungerade det att starta om datorn, men endast då det fanns en accesspunkt i närheten som den kunde få korrekta signaler från. Det felet lyckades vi aldrig lösa, men de kan ha berott på valet av drivrutiner för nätverkskortet. Detta upptäckte vi tyvärr inte förrän väldigt sent. Det gick dock ändå att samla in tillräckligt med data om nätverken för vår studie.

7.3. Sammanställning

För att slutligen sammanställa våra data så använde vi oss av programmet gpsmap, som kom med Kismet, med vilket vi kunde generera kartor över de nätverk vi lyckats upptäcka. Informationen på kartorna visar var nätverken fanns, deras utbredning och om de hade WEP aktiverat eller inte. För ytterligare information har vi gjort en närmare genomgång av Kissmets loggfiler ur vilka vi har sammanställt statistisk information om de upptäcka nätverken.

8. Resultat

8.1. Sammanfattning

Vi hittade fler nätverk än vad vi trodde vi skulle göra. Vi förväntade oss att vi skulle åka runt och hitta något då och då. Istället dök det upp nya nätverk hela tiden och totalt hittade vi 75 nätverk som vi kunde dokumentera.

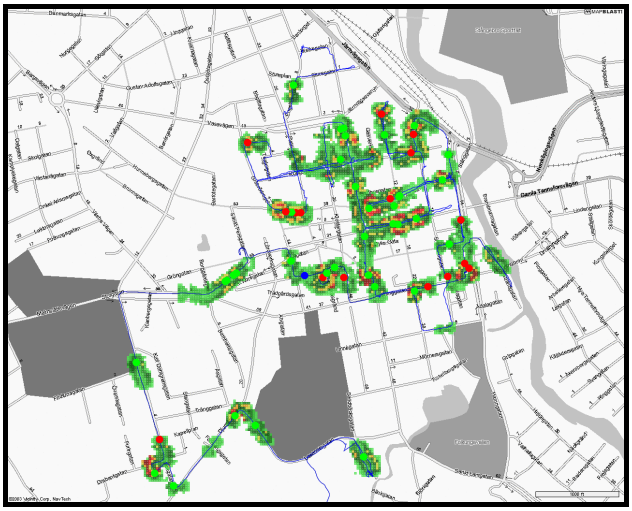
Endast en dryg tredjedel hade WEP påslaget. Detta var däremot inte särskilt oväntat. Att det dessutom var fler

nätverk i Mjärdevi som hade WEP påslaget var inte heller oväntat.

8.2. Kartor över upptäckta nätverk

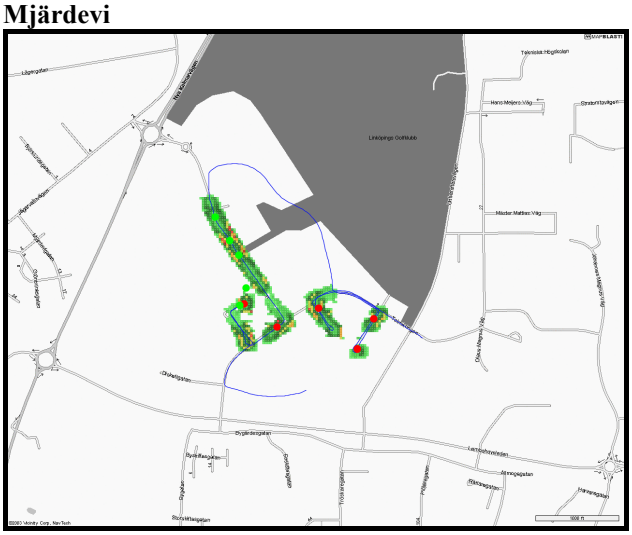
På nedanstående bilder är de nätverk vi har upptäckt utritade. En grön eller röd större punkt markerar var vi hade bäst signal från en viss accesspunkt. Det omkringliggande molnet visar nätverkets uppskattade räckvidd. Grön eller röd färg på punkterna visar om WEP ej är aktiverat respektive om det är aktiverat för den specifika accesspunkten. (Tyvärr vet vi inte vad den blå färgen på en punkt på centrumkartan betyder.) Den blåa linjen visar var vi har kört med bilen.

Centrum



(bättre bild kan ses på hemsidan)

Mjärdevi



(bättre bild kan ses på hemsidan)

8.3. WEP

Det första vi tittade på är om nätverken har WEP påslaget eller inte. Vi fann att följande gällde.

Totalt, i både centrum och Mjärdevi
Antal funna nätverk: 75 st
Antal där WEP är påslaget: 28 st (ca 37 %)
Antal där WEP inte är påslaget: 47 st (ca 63 %)

I centrum
Antal funna nätverk: 61 st
Antal där WEP är påslaget: 21st (ca 34 %)
Antal där WEP inte är påslaget: 40 st (ca 66 %)

I Mjärdevi:
Antal funna nätverk: 14 st
Antal där WEP är påslaget: 7 st (ca 50 %)
Antal där WEP inte är påslaget: 7 st (ca 50 %)

8.4. Summering

Totalt var det alltså drygt 1/3 av nätverken som hade WEP påslaget. Detta är ganska mycket, men inte alls oväntat. I centrum låg siffrorna än närmare 1/3 med WEP påslaget, medan 2/3 inte hade det. I Mjärdevi var det hälften som hade WEP påslaget. Vår gissning att det skulle finnas fler nätverk i Mjärdevi med WEP påslaget stämde alltså. Det var dock inte så stort antal företag i Mjärdevi som vi hittade. En anledning till detta kan vara att vi inte hade någon extern antenn till vårt nätverkskort och att det är längre avstånd mellan vägen som vi körde på och husen där företagen finns jämfört med vad det är i centrum. Hade vi t.ex. hittat sex accesspunkter till i Mjärdevi och dessa hade haft WEP (ett stort företag t.ex.) så hade siffrorna helt plötsligt blivit 2/3 med WEP i Mjärdevi. Det hade alltså varit säkrare siffror om vi hittat fler accesspunkter.

8.5. SSID

De tre vanligaste SSID var “default”, “homerun” och ”101” på respektive 11, 8 och 6 antal accesspunkter, följt av okänt SSID för 5 accesspunkter. Följande SSID fann vi där SSID inte var utbytt från tillverkarens standard:
”default” 12 st
"homerun" 8 st
”101” 6 st
”wireless” 2 st
”3Com” 1 st
“Linksys” 1 st

Vi har inte hittat dokumenterat att ”homerun” är ett default SSID, men vi anser att det är högst sannolikt med tanke på att vi hittade 8 stycken och att ”Telia homerun” levererar trådlösa förbindelser. Det är därför mycket troligt att det är just sådana som har default SSID "homerun". (Intressant att titta på vad Telia homerun själva skriver om säkerheten i trådlösa nätverk här: http://www.homerun.telia.com/swe/about/about_howitworks_security.asp. Intressant också att notera att inget

av nätverken med "homerun" som SSID hade WEP påslaget.)

Totalt visade sig alltså 30 st inte ha bytt ut default SSID. 6 accesspunkter hade stängt av SSID och det visades därför som okänt. Två hade SSID ”0 Unknown". Detta vet vi inte vad det är. Övriga 37 hade ett unikt eget SSID. Det var alltså ca 40 % som hade kvar defaultinställningen. Med våra knappa data för Mjärdevi var det dock nästan 50 % här som hade kvar defaultinställningen medan det var endast en dryg tredjedel i centrum.

8.6. Samband mellan SSID och WEP

Av de nätverken som inte hade bytt ut default SSID (30 stycken) hade större delen (24 stycken) inte heller slagit på WEP. Detta var också vad vi trodde innan vi undersökte nätverken. En betydligt större andel av dem som har bytt SSID har inte WEP påslaget jämfört de nätverk där SSID är utbytt. Det är endast ett fåtal nätverk där SSID fortfarande är inställt enligt defaultinställningen men där WEP är påslaget. Dock finns det några sådana nätverk. Det är svårt att säga någonting om skillnaderna mellan Mjärdevi och centrum när det gäller detta eftersom det handlar om ett sådant litet antal nätverk.

Vi hittade totalt sex nätverk som inte broadcastade någon SSID alls. Eftersom detta tyder på en säkerhetsmedvetenhet hade vi även förväntat oss att dessa nätverk skulle ha WEP påslaget. Det visade sig dock inte vara så. Mer än hälften av dessa nätverk hade WEP avslaget, vilket var något överraskande. Det är dock svårt att dra några egentliga slutsatser av detta, då det enbart handlar om några stycken nätverk.

8.7. Kanaler

Summering av kanalanvändningen:
Kanal 6: 26 st
Kanal 1: 17 st
Kanal 11: 9 st
Kanal 7: 8 st
Kanal 10: 6 st
Kanal 3: 3 st
Kanal 5: 2 st
Kanal 9: 1 st

Tre var av typen turbocell där vi inte känner till någon kanal.

En tredjedel av alla nätverk använder alltså samma kanal: kanal 6. Sedan är även kanal 1 väl använd. Förutom detta är det svårt att dra några slutsatser av detta. Bland de ofrekventa kanalerna finns båda accesspunkter med default SSID och sådana där SSID är utbytt. En gissning skulle annars kunna vara att om SSID inte är utbytt så är inte heller standardkanalen utbytt. Just kanal 6 är defaultkanal för många produkter.

8.8. Slutsatser

Det var inte oväntat att så få accesspunkter som 37 % hade WEP påslaget. Denna siffra är något högre än motsvarande i Stockholm eller i USA, där den antas ligga på 28 % respektive 20-25 % (enligt *Trådlöst osäkert*, ComputerSweden nr 93 2002 och http://www.enigma.ie/wardrive/right.php#wep). Det var inte heller oväntat att många accesspunkter inte hade bytt ut default SSID. Det som däremot var oväntat var att det fanns så många accesspunkter. I princip är ju hela centrum täckt, och detta är även då vi körde runt utan extern antenn med datorn instängd i en bil.

Det vi vet efter denna studie är vilka accesspunkter som inte använder WEP och har ett default SSID, vad vi dock inte vet är om det finns andra säkerhetsåtgärder implementerade på högre nivåer i dessa nätverk. Detta kräver vidare undersökningar för att ta reda på.

För att kunna dra några egentliga slutsatser gällande skillnaderna mellan centrum och Mjärdevi skulle en mer omfattande undersökning behövas göras. Underlaget är inte tillräckligt stort när det gäller antalet nätverk i Mjärdevi. Om fler nätverk skulle kartläggas där skulle även resultaten vara säkrare. Dock verkar det som att fler nätverk har WEP påslaget i Mjärdevi med det underlag som vi funnit i vår undersökning.

8.9. Förbättringar och förslag till fortsatt arbete

En klar förbättring hade varit att använda sig av en extern antenn till nätverkskortet. Detta hade utvidgat räckvidden och vi hade kunnat hitta inte bara fler nätverk utan möjligtvis också kunnat positionera de upphittade bättre. Vid en wardriving i Hong Kong upptäcktes fyra gånger så många nätverk då antenn användes jämfört med då antenn inte användes.

En fortsättning på arbetet kan vara att fokusera på något nätverk och försöka samla mer data från detta. Nu åkte vi runt och lät Kismet upptäcka nätverk och spara den data som Kismet kunde upptäcka. Vi hade även kunnat använda andra program. Kismet dög dock alldeles utmärkt till att upptäcka nätverken och ta reda på om de hade WEP eller inte. För de nätverk som hade WEP kan andra program användas för att prova att knäcka WEP-nycklarna. De nätverken utan WEP kan vara intressanta att undersöka närmare.

För en Internetversion av denna rapport besök http://wlan.no-ip.org där det även finns länkar till annan information inom området.