Universitet i Oslo
Institutt for informatikk

INF5251 V09

Midtveisrapport

Bluetooth Messaging Service

Kristian Sporsheim,
Rolf Erik Normann &
Karsten Jansen

13.03.2009

Innhold

Innledning

Hvordan kan vi utnytte blåtann i mobile enheter til å spre relevant informasjon til brukere?
Vi vil undersøke om brukere er interessert i å kunne motta relevant informasjon i forhold til den lokasjonen de befinner seg på. Dette kan være alt fra kinoer, musikk butikker, forretninger etc. Ved å utnytte den korte rekkevidden blåtann har, kan vi sende relevant informasjon til brukere som er innen riktig rekkevidde.

Vi vil undersøke hva som gjør blåtann til et aktuelt kommunikasjonsmedie for oss, og for brukerne. Dette går både på det tekniske og brukervennlige, samt villighet til bruk av tjenesten. Linjen mellom informasjon og spam kan være tynn. Hva ser brukerne som relevant informasjon?

Vi må undersøke om noen lignende prosjekter har blitt gjort før, eventuelt hva vi kan gjøre annerledes.

Det etiske aspektet er også viktig å utforske. Er det mulig å kunne misbruke denne teknologien? Vil det være noe å tjene på å misbruke den?

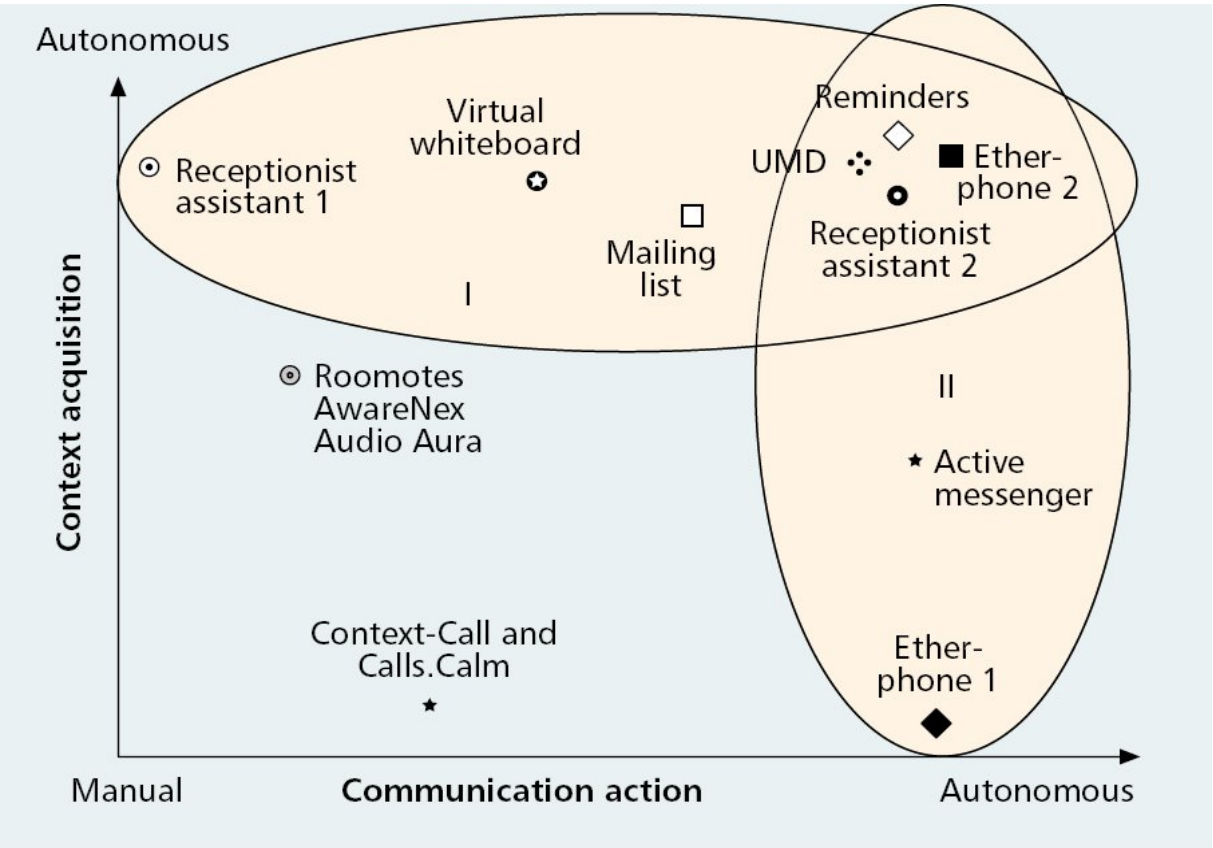
Vi ønsker å undersøke om blåtann er en teknologi som vil utvikle seg eller om det er andre teknologier som tar over, og hvor lenge den eventuelle prototypen vi lager kommer til å være aktuell. Vi vil også diskutere andre kommunikasjonsmedier som vi kunne ha brukt.

Metode

Pensumlitteraturen inneholder relevante artikler, og vi vil forsøke å trekke ut nyttig teori fra disse. Vi har planer om å lage en prototype i Python og vi kommer til å bruke Open Source biblioteker som Bluez, Bluez for Python og ussp-push. Når vi har en fungerende prototype, vil vi foreta testing av denne på forskjellige bruksområder. I sammenheng med denne vil vi foreta enkle intervjuer av forsøkspersonene.

Teori

"Context Aware Communication" Schilit, B.N., Hilbert, D.M., Trevor, J.
IEEE Wireless Communications • October 2002



Artikkelen "Context aware communication" forklarer hvordan context awareness, det å sette eller la applikasjoner sette og bruke informasjon om lokasjon, miljø, hvem som er i nærheten og hva man driver med, kan bedre kommunikasjon og bryte barrierer for kommunikasjon mellom grupper og individer. Artikkelen skisserer en måte å analysere kontekstsensitiv kommunikasjon gjennom to dimensjoner som strekker seg fra manuell til automatisk; context aquisition og communication action.

Context acquisition er måten systemet eller applikasjonen får kunnskap om en persons kontekst, det være seg lokasjon, miljø, sosialt e.l. En verdi nær "manuell" tilsier at et menneske, enten personen selv eller en operatør, må taste inn / angi verdier for konteksten. "Automatisk" betyr at systemet selv oppfatter / sanser konteksten. Et eksempel gitt i artikkelen kommer fra Olivetti, og deres Active Badge. Dette var en infrarød-sender festet på de ansatte, som lot sensorer i forskjellige rom sanse hvor den aktuelle personen befant seg.

Communication action dreier seg om hvordan systemet agerer på kontekstinformasjonen. Manuell her betyr at operatøren / brukeren selv bruker kontekstinformasjon til å bestemme og utføre en kommunikasjonshandling, for eksempel sende en faks til en lokasjon nær mottakeren. Automatisk betyr at systemet selv trekker ut relevant informasjon om kontekst, og velger en passende metode for kommunikasjonen. Et av eksemplene gitt i artikkelen handler om MIT active messenger, en applikasjon som prioriterte og videresendte epost ut ifra hvor man befant seg og hvilke aktiviteter man hadde skrevet inn i avtalebøker og lignende.

Artikkelen konkluderer med at det er vanskelig å automatisere begge prosesser – det er uhyre vanskelig å programmere "common sense", noe man mister hvis man sløyfer en menneskelig operatør.

Å automatisk samle info om kontekst er en stor utfordring, da det er umulig å vite hva som skjer i hodene på folk. Et system kan sanse at en person har vært stillesittende ved pulten sin en halvtime, men det er vanskelig å vite om personen dagdrømmer eller sitter i dyp konsentrasjon om en arbeidsoppgave.

Et annet viktig poeng er eventuelt tap av privatliv og personlig informasjon. Er folk villige til å ta i bruk teknologi som kan sanse hvor de er, hva de gjør og i ytterste konsekvens hva de føler og tenker? Hva om denne informasjonen kommer uvedkommende til veie?

Vi analyserer vårt eget prosjekt på de to dimensjonene context acquisition og communication action.

Context acquisition: Våre applikasjoner vil i første omgang befinne seg, og virke på, et gitt sted. Konteksten er på denne måten gitt på forhånd, men det faktum at en aktuell bruker befinner seg i denne konteksten er det interessante. Brukerenes blåtann-applikasjon vil fanges opp automatisk. Context acquisition gjelder altså bare lokasjon, men dette er realistisk sett det eneste vi er interessert i eller har mulighet til å fange opp.

Communication action: Vår applikasjon vil forsøke å sende info automatisk i dét den oppdager en blåtann-enhet. Handlingen er altså automatisk.

Vi ser at på et såpass ukomplisert system som vårt, vil begge dimensjoner kunne være automatisk. Det kan være interessant å tenke seg et mer komplisert scenario der systemet kjenner igjen brukeren basert på attributter som mac-adresse og navn på blåtann-devicen. Dette er ting som lett kan fanges opp. Dersom man har et register over brukere, vil man kunne lagre preferanser og brukshistorie, og på bakgrunn av dette sende tilpasset informasjon til brukeren.

Har man flere lokasjoner betjent av et system, kan man også finne bruksmønstre, og gi informasjon deretter.

Om folk er villige til å bruke disse systemene, og utsette seg for potensiell snusing i privat informasjon, er som nevnt tidligere ikke en selvfølgelighet.

Hva er gjort tidligere

En viktig del av forarbeidet i utvikling av nye løsninger er å gå igjennom hva som har blitt gjort tidligere i lignende prosjekter. En kan være så innovativ en bare vil, men sannsynligheten for at noe lignende er blitt gjort før, er meget stor.

DeliDeluca

Rett etter å ha levert undringsdokumentet fikk vi våres første overraskelse. På deli er det allerede et ferdig system i bruk som nettopp bruker blåtann teknologien til å sende informasjon til brukere. I enkelte deli butikker i oslo bruker de i dag blåtann for å markedsføre produkter eller markedsføre videoer med små videosnutter. Det fungerer på den måten at flatskjermene kontinuerlig viser de utvalgte produktene, og i tillegg foreslår at du slår på blåtann for å mota ”gode tilbud”. etter å ha aktivert blåtann får du etter kort tid en request om å ta imot en fil(video,flash, etc), som du kan spille av på din mobil.

BluAir

Når det gjelder markedsføring på mobil via blåtann fant vi fort ut at det var flere aktører som tilbyr ferdige løsninger. En av de mest profesjonelle aktørene vi kom over var BluAir.pl. Dette firmaet tilbyr hele løsninger, alt fra hardware desktop enheter og mobile enheter som er laget for å kunne opprettholde mange blåtann kontakter. Til ferdige web grensesnitt hvor du kan styre hva blåtann enheten skal sende ut til brukerne. Her kan du også følge med på statistikker etc.

Personal area network

Personal area network(PAN) er et nærhetsdatanettverk som kan brukes til kommunikasjon mellom for eksempel datamaskiner og telefoner. Det eneste kravet er at de deler samme teknologi og at de er i nærheten av hverandre. Enkelte teknologier krever at de må være innen synlig rekkevidde. En av grunnene til at man kaller det PAN er at rekkevidden sjelden er mer enn 10 meter, men enkelte teknologier har en rekkevidde opp til 100m. PAN kan brukes til kommunikasjon mellom seg selv(to eller flere enheter) eller for å koble til et høyre nettverk som er tilkoblet internett, skrivere og lignende. Kommunikasjon mellom enheter er ofte brukt til headsett, streame musikk, overføre filer, styre lys og mye mer.

Teknologier i PAN

PAN er ikke nødvendigvis trådløs, for ved bruk av USB eller firewire kan du enkelt sette opp ditt eget PAN nettverk. Mac brukere er godt kjent med bruk av firewire for å kunne overføre filer mellom to maskiner.
Når teknologien blir trådløs bruker man navnet Wireless personal area network eller WPAN(IEEE 802.15). Ved bruk av teknologier som IrDA, Bluetooth, UWB, Z-Wave og ZigBee kan man enkelt sette opp et WPAN, mens enkelte at teknologiene er mer utbredt enn andre.

Infrared Data Association

Infrared Data Association(IrDA) er en protokoll standard for å kunne overføre data over korte avstander ved at man bruker infrarødt lys. IrDA har veldig kort rekkevidde og må ha fri sikt til enheten den prøver og koble til. Hastigheten kan variere fra 2.4kbit/s til 16MBit/s, men det er færre og færre enheter som har IrDa siden den blir byttet ut med blåtann i de fleste enheter. Den største grunnen til dette er nok at det er umulig å sende data uten at man har frisikt under hele overføringen.

Ultra-wideband(UWB)

UWB er en radio teknologi som er veldig energi besparende med tanke på strøm. Teknologien brukes til korte avstander og har en høybåndbredde. UWB bruker en stor del av radio spektrumet, faktisk så bruker UWB en båndbredde på over 500MHz. Dette er fortsatt på forskingsstadiet og er ikke i kommersielt bruk i mobile enheter som mobiltelefoner og PDAer.

ZigBee

ZigBee er spesifikasjon som passer høynivå kommunikasjonsprotokoller ved at man bruker lavvolts digitalradio som baserer seg på IEEE 802.15.4-2006 standeren for WPAN.
Siden ZigBee har et veldig lavt effektforbruk så egner denne teknologien seg veldig bra til enheter med små batterier. ZigBee bruker *mesh networking*, som er en måte å rute pakker mellom noder som gir en høy **driftssikkerhet** og en lengre rekkevidde.

Bluetooth

Bluetooth, eller blåtann er en av de mest utbredt trådløse teknologiene i dag. De aller fleste har en eller annen enhet som har blåtann installert, om det er mobiltelefonen eller, hodetelefoner eller en bærbar pc. Blåtann er en trådløs protokoll for å utveksle data over korte distanser stasjonære og mobile enheter. Dette gjøres ved at man lager personalarea networks. Bluetooth har muligheten at den kan koble til flere enheter på en gang slik at man overkommer problemer med synkronisering. Rekkvidden på bluetooth er fra 1-100m avhengig av sender/mottaker.

Class	Maximum Permitted Power mW (dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

Bluetooth - Piconet

Piconet er navnet på Bluetooth PAN og kan bestå av 8 aktive enheter og kan ha veldig mange noder som er ”parkert”/ikke aktiv. Oppbygningen i piconet består av master og slave noder, der den første noden er master mens resten av nodene er slave og slave nodene kommuniserer med masternoden. Rekkevidden på et piconet er som regel 10m, men man kan lage nettverk på som har rekkevidde på 100m under perfekte forhold.

Bluetooth – Vårt prosjekt

Vi valgte blåtann som teknologi siden den er en av de mest utbredte innen for mobilenheter og datamaskiner. Samtidig er blåtann veldig godt implementert i de fleste operativsystemer og mobiltelefoner. Blåtann gjør det enklere for oss å implementere vår ide, siden vi kan bruke eksisterende blåtannprotokoller. En annen viktig faktor er den begrensende rekkevidden på blåtann som gjør at signalene holdes innenfor den aktuelle lokasjonen. Siden vi kun ønsker at brukere som er i den aktuelle lokasjonen skal få tilsendt informasjon som angår dem og ikke tilfeldig forbipasserende(F.eks utenfor en butikk).

Prototype - Bluetooth Messaging Service

Bluetooth messaging service er først og fremst en informasjons spreder som sprer informasjon i henhold til lokasjoner, som for eksempel kino, kantine, parkeringshus osv.
Er du på kino kan du få informasjon om eventuelle nye kinoer eller filmtrailere sendes til din mobil. En bruker kan alltid avslå en forespørsel og vil da ikke bli kontaktet på nytt. Tanken bak tjenesten er at det ikke skal være en form for irriterende reklame, men til informasjon for brukeren. Selv om skille mellom reklame og informasjon er målet vårt og ikke bli oppfattet som en reklame/SPAM.

Prototype – Utvikling

Vi undersøkte også andre programmeringsspråk og observerte at det var fult mulig å bruke Java og C, men dette krevde mye mer arbeid og gav ingen fordeler i ytelse eller funksjonalitet.

Dermed valgt vi å lage prototypen i Python grunnet gode støtte for blåtann under Ubuntu 8.10 og tilgangen til forskjellige biblioteker og programmer. Vi støtter oss på BlueZ, som er blåtann biblioteket for Linux og PyBluez som er pythonbiblioteket(utviklet på MIT) som er knytet opp til BlueZ. For å kunne sende data bruker vi ussp-push som er et lite program for å kunne sende filer via blåtann.

Python programmet kjører på en stasjonærenhet som skal søke etter enheter som har aktivert blåtann. Programmet skal da returnere en Media Access Control(MAC)adresse og navnet på enheten. Vi kan også bestemme hvor lenge vi skal søke etter enheter.
Et kode eksempel på dette er:

```
nearby_devices = bluetooth.discover_devices( duration = 4)#Scann i 4 sekunder
print nearby_devices
```

Eksemplet returnerer en liste med par: *[("00:1C:B3:33:B5:68", "Test")]* der enheten sitt navn er ”Test” og MAC adressen er 00:1C:B3:33:B5:68. Det er MAC adressen må vi ha for å kunne sende informasjon til enheten, men dette er ikke det eneste vi trenger.

For å kunne sende informasjon til en enhet trenger vi å få vite hvilke protokoller enheten har tilgjenglig. Blåtann er oppbygd slik at om en enhet er satt synlig, kan man spørre enheten om hvilke protokoller den har å tilby. Her er et forenklet kodeeksempel der vi bruker MAC adressen til enheten for å spørre enheten hvilke protokoller den har:

```
service_matches = bluetooth.find_service(address = nearby_devices[0])

for services in service_matches:
    print " Name: %s" % (services["name"])
    print " Host: %s" % (services["host"])
    print " Description: %s" % (services["description"])
    print " Protocol: %s" % (services["protocol"])
    print " Provider: %s" % (services["provider"])
    print " Port: %s" % (services["port"])
    print " Service id: %s" % (services["service-id"])
print ""
```

Dette gir oss en pen oversikt over de forskjellige protokollene blåtann enhetene har. Et eksempel på en protokoll er:

```
Name: OBEX Object Push
Host: 00:18:13:47:0A:7F
Description: None
Protocol: RFCOMM
Provider: None
Port: 6
Service id: E006
```

Det er nettopp ”OBEX Object push” vi kommer til å bruke for å kunne sende informasjonen vi ønsker via blåtann.

Prototype – Hva er ferdig?

- Skanne blåtann enheter og hente ut riktig informasjon
- Hente ut riktig port informasjon
- Manuell sending, delvis automatisk.
- Sende alle mulige filer

Prototype – Hva har vi igjen å gjøre?

- Lagre enheter som har mottatt melding, eller avslått meldingen.
- Automatisk sende filer helt uavhengig av enhet/port.
- Error handling. Slik at programmet ikke stopper opp om noe galt skjer, men heller prøver på nytt litt senere.
- Testing!

Blåtann sikkerhet

I de siste årene hvor populariteten for blåtann trådløs overføringsteknologi har steget, har også interessen for å missbruke teknologien økt proporsjonalt.

I 2003 ble det av Adam Laurie fra A.L Digital Ltd oppdaget mangler i autentisering av data overføring mekanismen i enheter med blåtann støtte.

I 2004 kom det første viruset som spredde seg fra mobil til mobil ved hjelp av blåtann, det trengte kun en godkjennelse fra brukeren for å bli installert. Og i 2005 kom mobilviruset ”Lasco.A” som var laget for symbian OS mobiler. Dette viruset installerte seg selv og spredde seg automatisk etter installasjon.

For å opprette en blåtann forbindelse mellom to telefoner blir det ofte brukt en blåtann ”PIN” som må bli tastet inn i begge enhetene for at en forbindelse skal bli opprettet.

De vanligste formene for blåtann angrep utnytter ofte blåtann arkitekturen, en kort PIN kode eller en svak implementasjon.

Det finnes en rekke metoder å angripe en telefon på gjennom blåtann teknologien, blueSnarf, blueBug, blueSmack, blueStab, blueBump, bluesnarf++, blueSpooof, blueDump, blueChop, bluePrinting, blueTooone, blooover.

Et bluesnarf angrep er et angrep som utnytter seg av en svak implementasjon i mange mobiltelefoner, spesielt OBEX protokollen. En kobler da opp med en OBEX push profil og gjør en OBEX GET request for kjente filnavn, og laster ned data fra enheten skjult. Et eksempel på dette skjedde i 2005 da milliardærarvingen Paris Hilton fikk mobilen sin hacket via blåtann, kontakt listen og mobilbilder stjålet og lagt ut på nettet.

4 entities for sikkerhet i blåtann
Alle blåtann enheter har en:
- Device addresse (BD_ADDR) som er unik (48bit)
- Private authentication nøkkel som er random (128 bits)
- Private encryption key (8-128 bit)
- (RAND) number, frequently changing (128 bit).

Vi lurer på

Vi lurer på om blåtann på mobil er en sikker teknologi i forhold til hva våres gruppe jobber mot. Hvilke måter er det muligheter det for eventuelt å missbruke dette. I forhold til vår prototype er det mest essensielle hvorvidt det er sikkert å ha blåtann aktivert på mobilen til en hver tid.

I takt med en blåtann teknologi som fornyer og forbedrer seg har også det ekstra strømforbruket ved å ha blåtann aktivert blitt kraftig redusert. I en uoffisiell test vi kontinuerlig har gjort, (henholdsvis på kollektiv transport) har vi funnet ut at det er et stort antall mennesker som går

rundt og har blåtann aktivert på mobilen til en hver tid. Hvem disse personene er og til hva de bruker blåtann til er ennå ukjent, men kan være noe vi burde undersøke videre i prosjektet.

Sikkerhets risikoer i forhold til blåtann som adgangskort på ifi:

- Det er mulig å clone en blåtann mac adresse ved med av PC
- Veldig lett å finne navnet på enheten
- Ikke like lett å få en PC til å se ut som en mobil, via blåtann
- Men ingen ting er umulig!
- Men kombinasjonen av disse tre er ikke like lett!
- Da er det kanskje like lett å knuse døra eller stjele et studentkort ;)

Konklusjon Sikkerhet

Det har vært mange angrep på blåtann i forbindelse med dårlig implementeringer og feil i arkitekturen, men slik vi ser det er blåtann fremtiden på vei til å bli en mer sikker teknologi. Vi vil videre i prosjektet undersøke hvorvidt det lar seg gjøre å implementere blåtann på mobil som adgangskort på ifi.

Etiske rammer

Vi må finne ut om vi holder oss innenfor de etiske rammene? Som vi nevnte i undringsdokumnetet, vil vi kontakte datatilsynet for å få et helt klart svar på hva som det er lovelig å gjøre innen blåtann teknologi i henhold til norsk lov.

Veien videre

Vi har noe igjen på prototypen og trenger en del brukertesting for å få ting å gå problemfritt. Først og fremst må vi få laget listen over enheter som har mottatt meldingen eller avslo meldingen, slik at vi ikke sender flere meldinger til disse. Dette er en viktig faktor for at vår tjeneste skal holde seg innenfor rammene for en informasjonsspreder og ikke en reklame tjeneste.

Problemet med blåtann er at hver produsent velger å implementere protokollen på litt forskjellige måte. Dermed krever det en del fra serverer siden for at vi skal kunne sende meldinger helt automatisk uten å måtte gjette hvilke port protokollen kjøre på.

Errorhandling er en av de tingene vi må se på for å få flyt i programmet. Vi veldig avhengig av at programmet ikke stopper opp selv om det støter på uforutsigbare elementer og heller skriver disse i en loggfil.

Sist men ikke minst, så trenger vi en del brukertesting for at programmet skal kunne kjøre uten problemer, men også for å hente inn informasjon fra brukeren om hva de synes om prototypen.

Vi trenger også å hente inn mer teori fra en ny forskingsartikkel som vi kan hente relevant teori og få inspirasjon.

Referanser

http://www.thebunker.net/resources/bluetooth
http://www.iki.fi/jiitv/bluesec.pdf
http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf
http://trifinite.org/
http://www.bluair.pl/
http://en.wikipedia.org/wiki/Bluetooth
http://en.wikipedia.org/wiki/Personal_Area_Network
http://en.wikipedia.org/wiki/IEEE_802.15
http://en.wikipedia.org/wiki/Ultra-wideband
http://en.wikipedia.org/wiki/ZigBee
http://www.bluez.org/about/
http://org.csail.mit.edu/pybluez/index.html
http://xmailserver.org/ussp-push.html
http://www.ieee802.org/15/

Schilit, B., Hilbert D., Trevor, J.: *Context-Aware Communication*, 2002. IEEE Wireless Communications.