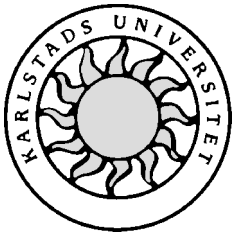

Datavetenskap

Opponenter:

Reza Javanbakhti

Jimmy Pesola

Respondenter:

Anders Heimer

Jonas Seffel

Säkerhetsanalys av Bluetooth-kommunikation

Oppositionsrapport, C-nivå

2006:09

1 Sammanfattat omdöme av examensarbetet

Respondenterna har gjort ett bra jobb med examensarbetet. Innehållet i uppsatsen har bra sammanhang och ett lärorikt och intressant innehåll. Resultatet med examensarbetet var också bra, då det visade att vanliga mobiltelefoner utrustade med Bluetooth kan var sårbara för olika typer av attacker.

2 Synpunkter på uppsatsen knuten till examensarbetet

Uppsatsen hänger bra ihop med examensarbetet, d.v.s. uppsatsen täcker väl det som examensarbetet handlar om.

2.1 Titel

Titeln till uppsatsen stämmer väl överens med examensarbetet. Examensarbetet handlar just om att undersöka säkerheten i enheter utrustade med Bluetooth.

2.2 Uppsatsens disposition

Dispositionen i uppsatsen är logisk och har bra sammanhang. Det finns ett par strukturella fel vid vissa tillfällen där det nämns ett begrepp och det förklaras inte alls om vad det är för något, men man hänvisas framåt i uppsatsen för en förklaring. I övrigt så är uppsatsens struktur mycket tydlig och den röda tråden är lätt att följa.

2.3 Begreppsapparat

De flesta begrepp som används i uppsatsen är bra förklarade, men i vissa fall hade det varit bra med åtminstone en förklaring till vad en förkortning står för direkt där begreppet nämns för första gången. Ett exempel på detta är i en mening där en förkortning nämns för första gången i uppsatsen: ”Värden står för L2CAP-lagret samt andra övre lager som kan behövas.” Meningen är citerad ur avsnitt 2.2.1 på sidan 5. Ett annat exempel som inte fick någon förklaring var ”business card exchange” i avsnitt 2.2.4 på sidan 15. I kommentaren till figur

3.1 och figur 3.2 på sidan 21 respektive sidan 22 påstås det att figurerna är sekvensdiagram, men i själva verket är de flödesscheman.

2.4 Argumentering och slutsatsdragning

Argumenteringen och slutsatsdragningen är bra. I alla argument finns det tillräckliga grunder och hänvisar till litteratur i de fallen där det behövs.

2.5 Sammanfattningen

Det som anses vara en sammanfattning är det som står i kapitel 6 med rubriken ”Slutsats”. Sammanfattningen av uppsatsen är bra skriven. Den tar med alla aspekter av den undersökning som respondenterna har gjort, och går inte in för mycket på detaljer.

2.6 Språkbehandling

I sin helhet var uppsatsen bra skriven när det gäller språket. Dock fanns det ett par särskrivningar och hopskrivningar, onödiga ord och på något ställe var det en lång mening med flera bisatser vilket ledde till en konstig ordföljd.

2.7 Referat och källförteckning

Vissa referenser har skrivits på ett felaktigt sätt. Det finns ställen där en referens ingår som ett ord i meningen där referensen finns. Referenser ska endast vara metatext och markera ett enstaka begrepp att det finns en referens till det. Ett korrekt exempel ur uppsatsen är ”…att räkna fram nyckeln inom rimlig tid enligt Gehrmann [8]”, men t ex vid ett tillfälle i texten har de skrivit fel på följande sätt ”I [23] skriver Potter att …”. Referenserna i källförteckningen var inte korrekt ordnade i vissa fall. De referenser som innehöll namnet på en eller fler personer var korrekt ordnade emellan varandra, men andra referenser så som länkar till hemsidor och namn på företag var däremot inte korrekt ordnade. Ett exempel på detta är ”[1] Infrared Data Association. Welcome to IrDA. Se http://www.irda.org/.”. Även i avsnitt 4.3.1 finns det två hänvisningar till figurer, Figur 4.3.1 och Figur 4.3.2. Figurnumreringen stämmer inte överens med dessa hänvisningar.

2.8 Övriga kommentarer

Uppsatsen har inte följt mallen som finns på hemsidan för examensarbetet.

3 Genomgång av uppsatsen kapitelvis

3.1 Kapitel 1

I Avsnitt 1.2 var syftet väl formulerat, men det står inte så mycket om målsättningen. Allt annat i kapitlet var bra.

3.2 Kapitel 2

Det finns en hänvisning som inte existerar, ”Se avsnitt 2.3 för en genomgång av protokollstacken.”, i avsnitt 2.2.1 på sidan 5. Denna hänvisning finns också en gång tidigare i avsnittet. Hänvisningen syftar på begreppet ”L2CAP”, som inte förklaras innan hänvisningen till avsnitt 2.3. I övrigt är alla andra begrepp bra förklarade innan en hänvisning görs för ytterligare detaljer.

I avsnitt 2.2.2 på sidan 6 står det ”Bluetooth-kommunikation sker i så kallade ad hoc-nätverk. Detta innebär att ett nätverk av enheter kan skapas var som helst och när som helst.”. Det som inte framgår i denna mening är vad som menas med ”var som helst och när som helst”.

I avsnitt 2.2.2 beskrivs situationer där flera enheter ingår i minst två piconät, så ”…kallas de piconäten tillsammans för ett ’scatternet’.” Här skulle det också kunna beskrivas om hur relationerna master och slave fungerar mellan två olika piconät.

I avsnitt 2.2.3 på sidan 10 står det ”IrOBEX är ett protokoll för att skicka dataobjekt som kalenderinformation, e-post och mycket mer.”. Det hade varit bra om alla dataobjekt hade nämnts, alternativt att referera till den bok eller hemsida där respondenterna har hittat informationen.

I avsnitt 2.2.3 finns det ett begrepp som har onödiga citattecken, ”’telephony control’-protokollet”. Detta kan skrivas utan citattecken. Även citationstecknen i meningen ”Gruppen är inte bara ’bakåt kompatibel’…”, som finns i samma avsnitt, är onödiga. Det finns en mening i detta avsnitt som skrivits otydligt, ”Rent tekniskt ingår inte applikations-gruppen i protokollstacken, utan den använder sig av den.”. I det här fallet vet man inte vad ”den” syftar

på. Vid några tillfällen nämns begreppet ”luftgränssnitt”, och det finns ingen förklaring till vad begreppet betyder, och vad det innebär att initiera ett luftgränssnitt.

I avsnitt 2.2.3 på sidan 12 står det: ”Bluetooth delas in i tre kraftkategorier:

- Kategori 1: klarar en räckvidd på c:a 100, sändningskraft – 20 dBm.
- Kategori 2: klarar en räckvidd på c:a 10m, sändningkraft – 4 dBm.
- Kategori 3: klarar en räckvidd på c:a 0.1m, sändningskraft – 0 dBm.”

Referensen som anges i slutet av punkten refererar inte direkt till innehållet där denna information finns. Det var svårt att hitta informationen, eftersom den inte fanns direkt tillgänglig i referensen, och man var tvungen att söka efter den.

Begreppet ”’business card exchange’” behöver förklaras närmare i avsnitt 2.2.4 på sidan 15.

I avsnitt 2.2.4 på sidan 16 finns det en mening som har en oklar betydelse, ”Profilen kräver användning av autentisering och kryptering istället för interaktion med användaren som ett skydd.”. Detta kan tolkas som att interaktion med användaren inte görs överhuvudtaget när autentisering och kryptering används, eller tolkas som t ex att interaktion med användaren är ett skydd.

I avsnitt 2.2.4 på sidan 15 står det ”För att minimera riskerna med filöverföring kräver FP att en användare måste acceptera varje sändning och mottagning.” men det nämns inte vilka risker det handlar om. I samma avsnitt på sidan 16 står det ”För att undvika att personer som inte har rätt att utnyttja gatewayen blir en del av piconätet så måste alla enheter autentiseras.”. Vad som menas med att personer blir en del av piconätet är inte tydligt. Och ”gateway” är inte ett svenskt ord och kan därför inte böjas enligt svenska grammatiska regler.

I avsnitt 2.2.4 på sidan 18 står det ”LAN:et”. Här hade lokala nätverket passat bättre, eftersom man inte kan böja ”LAN” med svenska grammatiska regler.

Kapitel 2 är ett ganska långt kapitel i förhållande till andra kapitel i uppsatsen, och de flesta felen hittade vi i detta kapitel. Men i övrigt är innehållet och strukturen i kapitel 2 bra.

3.3 Kapitel 3

Detta kapitel var ett av de mer intressanta avsnitten. Det mesta var väl beskrivet och lättförståeligt. Det fanns dock några fel som vi kände att vi måste anmärka på.

På sidorna 21 respektive 22 finns det två figurer som påstås vara sekvensdiagram, men i själva verket liknar de mer flödesscheman.

I avsnitt 3.2.1 på sidan 27 i figur 3.7 finns det två förkortningar som inte förklaras, ”LSB och MSB”.

I avsnitt 3.2.1 på sidan 28 står det ”Om sex paket totalt avlyssnas och de 2^{22} möjliga avsändaradresserna för varje paket jämförs får man fram en unik enhetsadress som med mer än 99% sannolikhet är den rätta.”. Det hade varit bra med en referens här.

I avsnitt 3.2.3 på sidan 29 behöver begreppet ”elektroniska visitkort” förklaras närmare.

I avsnitt 3.2.4 på sidan 30 nämns begreppet ”L2CAP”, och det måste finnas en referens eller en hänvisning där.

I avsnitt 3.2.4 på sidan 31 refereras Gianluigi två gånger, men det räcker att referera en källa en gång per kapitel.

I avsnitt 3.2.4 på sidan 31 står det ”…källdatan är större än den allokerade positionen i minnet där källdatan placeras…”. Detta är inte korrekt, eftersom data aldrig lagras i en position, utan i det allokerade minnet vid en position.

I avsnitt 3.2.5 på sidan 31 bör ”E_0” hänvisa tillbaka till avsnitt 3.1.3.

I avsnitt 3.2.6 på sidan 32 står det att viruset Pbstealer, som använder Bluetooth för att sprida sig, stjäl telefonboken och skickar sedan iväg den med hjälp av Bluetooth. Detta borde specifieras lite mer, t ex hur och till vem eller vilka skickas telefonboken.

I avsnitt 3.3 finns det ett exempel som förklarar hur en angripare kan ta reda på om en person är länkad till en viss Bluetooth-enhetsadress genom att ta reda på när den personen har med sig en Bluetooth-enhet då denne gör ett kreditkortsköp. Det är oklart hur enhetsadressen länkas till personen i fråga.

3.4 Kapitel 4

I avsnitt 4.1 på sidan 35 nämns operativsystemen Windows XP och Symbian, men de saknar referenser.

I avsnitt 4.3.1 på sidan 37 så nämns fel figur två gånger, figur 4.3.1. Figuren heter 4.1 i den första benämningen, och 4.2 i den andra benämningen.

I avsnitt 4.4 beskrivs det att funktioner i ”Phone.java” lagrar data i ”PhoneData-klassen”. Det framgår inte hur detta kan sparas i klassen. Om det handlar om statiska medlemmar i klassen, så är det korrekt. Annars borde det stå att det lagras i objekt av klassen ”PhoneData”.

3.5 Kapitel 5

Kapitlet var väl skrivet och bra strukturerat. Vi hittade inget som vi kunde anmärka på.

3.6 Kapitel 6

I avsnitt 6.1 står det ”Detta beror på att Bluetooth-standarden har funnits sedan år 1998 och tillverkare som implementerar Bluetooth-produkter har lärt sig av sina misstag.”. Det framgår inte i texten vilka misstag det handlar om. Om det inte är en slutsatsdragen av respondenterna, så måste det finnas en referens som förklarar vilka misstag det handlar om.

I avsnitt 6.3 påstås det att om programmering påbörjas innan en undersökning gjorts om ett visst bibliotek, så medför detta ofta problem. Det är otydligt vilka slags problem det medför om läsaren inte är insatt i ämnet.

3.7 Övriga kommentarer

I sin helhet har uppsatsen bra och intressant innehåll. I kapitel 3 förklarades säkerhetsriskerna och olika typer av attacker utförligt och på ett intressant sätt. I bilagan finns en tydlig anvisning till hur man kan vidareutveckla Bluetooth-sniffern. Denna anvisning var ett mycket bra tillägg ifall någon skulle vilja implementera fler testmetoder i sniffern.

4 Slutliga kommentarer

Uppsatsen är väl skriven och bra planerad. Innehållet i uppsatsen är relevant och har bra sammanhang. Kapitel 2 var lite rörig eftersom det finns några förkortningar och begrepp som inte förklaras helt, vilket gör det lite svårt att förstå innehållet i kapitlet. I övrigt är det bra att Bluetooth förklaras och hur det fungerar. Respondenterna har valt ett intressant ämne att göra ett examensarbete på, och det är också relevant i hög grad att göra en sådan undersökning som respondenterna har gjort.