EKONOMIHÖGSKOLAN
Lunds universitet

Mobilbetalningar med NFC

Användarnas syn på säkerhet

Kandidatuppsats, 15 högskolepoäng, SYSK01 i informatik

Författare
Felix Hulthén
Johan Lindström

Framlagd
2011-06-01

Handledare
Anders Svensson

Examinatorer
Lars Fernebro
Markus Lahtinen

Titel: Mobilbetalningar med NFC – Användarnas syn på säkerhet

Författare: Felix Hulthén & Johan Lindström

Utgivare: Institutionen för Informatik

Handledare: Anders Svensson

Examinator: Lars Fernebro

Markus Lahtinen

Publiceringsår: 2011

Uppsatstyp: Kandidatuppsats, 15 högskolepoäng

Språk: Svenska

Nyckelord NFC, mobilbetalning, RFID, kontaktlöst, säkerhet, attack

Abstract

Cash and credit cards are no longer considered to be the obvious methods of payment. During the last ten years mobile payments has been predicted as the next method of payment. Many methods exist but none of them has managed to become the standard way of paying. NFC, a further development of the RFID-technology, has been seen as the strongest contestant in the field. Security is considered to be one of the most important factors for consumers to adopt the technology and abandon current payment standards. There are some threats against the use of NFC, which in this paper are presented and evaluated through both existing literature and user perspective. The users' views on the security issues are assessed by conducting a survey. The result of the study shows that consumers value security and integrity as the most important factors regarding mobile payment. Furthermore, the threats are considered to be serious, which could prove to be a major hindrance concerning the future use of NFC-technology as the standard way of payment and a big step towards a cashless society.

Innehållsförteckning

Figur- och tabellförteckning

Förord

Vi vill tacka alla inblandade som på ett eller annat sätt bidragit till att göra denna rapport möjlig. Framförallt vill vi tacka de som svarat på vår enkät, samt vår handledare Anders Svensson.

Lund 2011-06-01

Felix Hulthén & Johan Lindström

1 Inledning

I detta kapitel redovisas bakgrunden till studien. Vidare redovisas problemområdet, syftet med studien och vår frågeställning, samt avgränsningar vi valt att göra. Slutligen definieras ett antal begrepp som förekommer i teorin.

1.1 Bakgrund

Ny teknologi ger användare möjligheten att betala med hjälp av mobiltelefoner och andra mobila enheter. Att betala med kontanter och kreditkort är inte längre en självklarhet, då man främst i Japan, Sydkorea och andra asiatiska länder redan kan betala med mobiltelefoner i butiker och i kollektivtrafiken. (Ondrus & Pigneur, 2009)

Mobilbetalningar har varit ett aktuellt ämne redan sedan början av 2000-talet. Världen över har det genom åren introducerats en mängd olika mobilbetalningstjänster, bl.a. betalning med hjälp av internetbanker och andra elektroniska betalningar. Nästan alla försök med mobilbetalningstjänster har misslyckats och den största delen av dessa tjänster har lagts ner. (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008)

NFC (Near Field Communication) är en vidareutveckling av RFID-teknologin, och använder trådlös kortdistans-teknik, med avstånd på ca 4 cm. NFC-kommunikation involverar alltid en sändare och en mottagare. Sändaren skickar radiovågor till en passiv mottagare. Således kan mottagarna vara av enkel karaktär i form av ”taggar”, klistermärken eller kort, som inte behöver en egen strömkälla i form av batteri eller liknande. Kommunikation mellan två peers (p2p) är också möjlig där båda enheter är strömförsedda. (NFC Forum, 2011)

NFC-försedda mobiltelefoner förutspås uppgå till 863 miljoner enheter till 2015 och kommer ha mer än 50 % av marknaden. Vidare spår man att NFC kommer att vara den ledande teknologin inom betalning med mobiltelefon och att värdet på betalningar globalt kommer att uppnå ca 111 miljarder euro. (Frost & Sullivan, 2011)

Eftersom NFC-teknologin främst används för mobila betalningar så är säkerhet en viktig aspekt. Det är viktigt att utveckla verktyg och tekniker för att försäkra sig om att mobilbetalningar kan genomföras så säkert som möjligt. (Mulliner, 2009)

Dessutom så bidrar den trådlösa kommunikationen till att säkerhetsrisker uppstår och attacker sker. Eftersom kommunikationen är kontaktlös kan attacker ske utan användarens vetskap, och att attackera en NFC-enhet är fördelaktigt då teknologin främst används till betalningar och transaktioner. (Madlmayr, Langer, Kantner, & Scharinger, 2008)

1.2 Problemställning och motivering

Denna uppsats behandlar risker och hot med kontaktlös mobilbetalning med NFC-teknologin ur ett användarperspektiv. Vi koncentrerar oss på frågorna om säkerhet och integritet, samt hur medvetna användarna är om och hur de värderar dessa aspekter vid mobilbetalningar. Eventuella hot kartläggs, varför de hoten finns och hur de hoten kan påverka eller skada användaren. En mängd litteratur diskuterar säkerhetsaspekten inom NFC och mobilbetalningar, men det finns ytterst lite litteratur som fokuserar på användarens syn på säkerhet. Som informatiker ser vi användarens synpunkter som avgörande beträffande denna nya teknologi, och vill därför ha denna utgångspunkt i vår studie. Vår forskningsfråga är således:

Hur medvetna är användarna om säkerhetsrisker inom mobilbetalning med NFC? Hur värderar användarna dessa risker?

Utifrån användarnas åsikter om säkerhet vill vi också få svar på följande följdfråga:

Kan säkerhetsaspekten vara ett hinder för NFC-teknologins framtida utveckling och spridning?

1.3 Syfte

Syftet med denna forskningsbaserade undersökning är att få kunskap om de verkliga hot och risker som finns stämmer överens med den enskilda användarens uppfattning. Vårt bidrag till informatik blir således i form av en utvärdering av säkerhet inom kontaktlösa mobilbetalningar och NFC, ur ett användarperspektiv.

1.4 Avgränsningar

Vad gäller avgränsningar inriktar vi oss enbart på NFC med mobilbetalningar i fokus, inte alternativa möjliga framtida betalningslösningar. Undersökningen är enbart inriktad på hot och säkerhetsaspekter ur användarsynpunkt. Det finns andra faktorer än säkerhet att beakta så som användarvänlighet, kostnad och liknande. Dessa faktorer behandlar vi endast i relation till säkerhet.

Med mobilbetalningar avses betalning med en mobil enhet, oftast en mobiltelefon. NFC-teknologin har många användningsområden inom betalning, t.ex. mellan två personer eller med en konsument och en automat. De betalningar vi behandlar är den traditionella handeln; med en konsument samt en försäljare på en fast plats, dvs. klassisk butikshandel.

Vår hypotes är att yngre människor är de första att anamma ny teknologi, har mycket kunskap i ämnet och således relevanta argument för sina åsikter. Därför är studien främst fokuserad på denna åldersgrupp.

1.5 Definition av begrepp

Definitioner och begrepp som är viktiga i uppsatsen:

- *DoS-attack* innebär att någon försöker hindra användarna från att få tillgång till en tjänst eller information. DoS står för Denial of Service och precis som namnet antyder innebär det att användaren vägras tillgång till tjänsten. (US-CERT, 2009)

- *Internetplånbok* kallas också för e-wallet och digital wallet. En internetplånbok kan liknas vid en fysisk plånbok men är digital och möjliggör elektroniska transaktioner. (Taghiloo, Ali Agheli, & Reza Rezaeinezhad, 2010)

- *Mobilbetalning* är en betalning med en mobil enhet, vanligtvis med en mobiltelefon eller en handdator. (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008)

- *NFC (Near Field Communication*) är en vidareutveckling av RFID-teknologin, och använder trådlös kortdistans-teknik, med avstånd på ca 4 cm. (Madlmayr, Langer, Kantner, & Scharinger, 2008)

- *NFC Forum* är en icke-vinstdrivande branschorganisation som grundades 2004 av Philips, Sony och Nokia för att utveckla och främja utvecklingen och implementeringen av NFC-teknologin, för att bl.a. säkerställa kompabiliteten mellan enheter och tjänster. NFC Forum vill hitta en gemensam global lösning för betalning med mobila enheter. (NFC Forum, 2011)

- *Phishing (nätfiske)* är ett försök att stjäla användarnamn, lösenord, kontoinformation och annan känslig information från användare. En metod för att göra detta kan vara att bedragaren skickar e-mail som ser ut att komma från exempelvis en bank eller en annan finansiell institution. (Yu, Nargundkar, & Tiruthani, 2008)

- *POS (Point of Sale)* är ett allmänt förekommande begrepp inom handelssektorn. POS är i sin enklaste mening en kassaapparat där betalningen sker i en butik eller restaurang. (Valcourt, Robert, & Beaulieu, 2005)

- *RFID (Radio Frequency Identification*), alltså identifikation med hjälp av radio-teknologi. RFID-teknologin har bl.a. ersatt traditionell läsning av streckkoder. (RFID Journal, 2011)

- *RFID-tag* är ett mikrochip med ett unikt identifikationsnummer och eventuell annan information. Taggen kan läsas och skrivas till med hjälp av radiovågor. Det finns passiva och aktiva taggar. En aktiv har egen strömkälla medan en passiv saknar detta och fungerar som en spegel. En del taggar innehåller permanent information och kan

således inte modifieras, medan andra kan programmeras med ny information. (RFID Journal, 2011)

- *Smart card* är ett kort i fickstorlek som innehåller en eller flera kretsar och läses av genom magnetremsa, streckkod eller kontaktlöst genom radiovågor. Vanliga bankkort är en typ av smart card. (Husemann, 1999)

2 Litteraturgenomgång

I detta kapitel följer vår litteraturgenomgång. Denna består av teorier som berör mobilbetalningar, metoder för dessa samt användaracceptans. Vidare presenteras relevant forskning om säkerhet inom mobilbetalningar. Slutligen ger vi en överblick över NFC och hot och attacker mot teknologin.

2.1 Mobilbetalningar

En mobilbetalning innebär en betalning för varor eller tjänster med hjälp av en mobiltelefon eller PDA (Personal Digital Assistant). Denna möjliggörs genom utnyttjandet av trådlös eller annan kommunikationsteknologi. Vidare definieras en mobilbetalning som en betalningstransaktion där pengar överförs från betalaren till mottagaren med hjälp av en mobil enhet. Detta kan ske med eller utan en mellanhand. Mobilbetalningar förväntas användas inom all försäljning i framtiden. (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008; Mallat, 2007; Valcourt, Robert, & Beaulieu, 2005)

Mobilbetalningar har blivit aktuellt pga. ett flertal orsaker. Bland dessa kan nämnas ett allt mindre användande av kontanter vid betalning, samt den snabba utvecklingen av mobiltelefonen och teknologin bakom telekommunikation. Det utbredda användandet av mobiltelefoner och mobiltjänster, såsom ringsignaler och applikationer, ligger också till grund för att mobilbetalningar är av stort intresse. (Mallat, 2007; Valcourt, Robert, & Beaulieu, 2005)

2.1.1 Mobilbetalning - metoder och scenarion

SMS-betalning
Enligt Mallat (2007) är betalning med hjälp av SMS i dagsläget den vanligaste mobilbetalningsmetoden i Europa. En SMS-baserad betalningsmetod innebär att konsumenten uppger sitt mobiltelefonnummer för att genomföra en transaktion, vilken sedan betalas via mobiltelefonräkningen. Som ett första steg i en sådan betalning skriver kunden in sitt mobiltelefonnummer på en webbsida. Kunden mottager sedan en transaktionskod via SMS, och koden anges sedan på webbsidan. En bekräftelse på transaktionen skickas sedan till kunden via SMS, och kostnaden läggs på mobilräkningen. (Valcourt, Robert, & Beaulieu, 2005)

Betalningen kan också genomföras genom att kunden skickar ett premium SMS, dvs. ett SMS till en fast kostnad som läggs på mobiltelefonräkningen. (Hard, Farahat, & Ezz, 2008). Fördelarna med SMS-betalningar är att den är säker och snabb. Vidare krävs inget kreditkort av kunden, och ingen teknisk utrustning hos försäljaren. (Valcourt, Robert, & Beaulieu, 2005)

Point of Sale (POS) mobilbetalning
POS-mobilbetalning innebär att kunden betalar på ett fast transaktionsställe med sin mobiltelefon. Kundens mobiltelefon synkroniseras med försäljarens enhet för att en transaktion ska ske. Transaktionsstället kan vara antingen en säljare eller en automat. (Valcourt, Robert, & Beaulieu, 2005; Pedersen, Hedegaard, & Sharp, 2006; Pousttchi, 2008)

Person-till-person (P2P) mobilbetalning
Med hjälp av P2P-betalning kan en transaktion mellan två personer äga rum. Oftast sker betalningen genom en tredje part, som t.ex. PayPal eller andra internetplånböcker. (Abdulhamid & Hattab, 2008; Valcourt, Robert, & Beaulieu, 2005)

Mobilbetalningar går också under samlingsnamnet m-commerce. M-commerce innebär att konsumenter kan köpa varor och tjänster med sin mobiltelefon oavsett var de befinner sig. (Hanebeck & Raisinghani, 2003) Således kan i princip all handel med mobiltelefoner hamna under detta begrepp, som t.ex. betalning med kontokort (via webbläsaren), samt betalning med diverse internetplånböcker.

2.1.2 Användaracceptans och TAM

För att visa vilka aspekter som är viktiga vid användaracceptens kan TAM (Technology Acceptance Model) användas. TAM är ett teoretiskt ramverk som är tänkt att bestämma användarnas vilja att använda ett nytt system eller IT. Ursprungligen bygger TAM på två faktorer: upplevd nytta och upplevd användbarhet. (Davis, Bagozzi, & Warshaw, 1989)

Upplevd nytta handlar om hur pass mycket individens arbetsprestation förbättras med hjälp av användningen av en viss teknologi. Upplevd användbarhet bygger på individens uppfattning om hur mycket ett visst system eller en teknologi kan komma att underlätta hans eller hennes arbete. Den upplevda användbarheten definieras i hög grad av den upplevda nyttan blir för individen. (Davis, Bagozzi, & Warshaw, 1989)

TAM har sedan vidareutvecklats och fler faktorer har tillkommit efter hand. Dahlberg et al. (2008) har sammanställt samtliga faktorer som tagits upp i annan litteratur. Sedan har dessa faktorer analyserats och de faktorer som har förekommit oftast har lyfts fram som viktigast när det gäller ny teknologi för mobilbetalningar. Dessa faktorer är: *användarvänlighet*, *pålitlighet och säkerhet*, *användbarhet*, *kostnad* samt *kompabilitet.* (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008)

Det finns olika åsikter om huruvida kön påverkar användarnas vilja att acceptera ny teknologi. Li, Glass & Records (2008) har i en studie visat att det inte är någon skillnad på mottagligheten av mobilbetalningar hos män och kvinnor. Andra studier visar emellertid att det finns en skillnad mellan könen. Su & Li (2010) fann att män har ett större intresse när det gäller nya funktioner och mer avancerad teknologi vid val och användande av mobiltelefoner, medan kvinnor mer använder mobiltelefonen efter hur användbar den är. Vidare finns det

forskning som pekar på att män generellt är mer benägna att ta risker än kvinnor. (Shivraj & Vikas, 2008)

2.1.3 Mobilbetalningar – säkerhet

Kundernas brist på förtroende gällande teknologi, återförsäljare och mobilbetalningar i allmänhet har visat sig vara ett stort hinder för mobilbetalningens framfart. (Siau, Sheng, Nah, & Davis, 2004)

I ett projekt undersöktes internetbaserade betalningstjänster för att identifiera vilka kriterier ett betalningssystem skulle uppfylla för att vara effektivt. För att hitta effektivitetskriterier inledde man med att undersöka vilka de huvudsakliga intressenterna är i ett betalningssystem. Med hjälp av enkäter tillfrågades ett flertal experter på området. Med hjälp av frågor försökte man bl.a. få svar på vilka effektivitetskriterier som ansågs som mest viktiga av involverade intressenter. (Shon & Swatman, 1998)

Enligt Shon & Swatman (1998) är konsumenten den viktigaste intressenten i ett betalningssystem då det är denne som måste se fördelarna med tjänsten för att överhuvudtaget använda den. Utan ett kundintresse finns inget behov av ett betalningssystem. De viktigaste effektivitetskriterier man fann i undersökningen var accepterbarhet, support, transaktionstid, användbarhet, flexibilitet, kostnader, integritet, tillförlitlighet och säkerhet. Vidare i studien så bad man alla intressentgrupper att rangordna effektivitetskriterierna för varje grupp. Man fann att säkerhet och tillförlitlighet var viktigast för alla intressentgrupper. Eftersom vår egen rapport handlar om användarnas syn på säkerhet lägger vi enbart fokus på dessa delar.

Det finns ett flertal krav för en säker elektronisk transaktion. Gollman (2011) och Shon & Swatman (1998) har beskrivit dessa och vi har i denna rapport belyst de vi finner viktigast för att besvara vår forskningsfråga, dvs. de krav som är eller kan vara direkt kopplade till mobilbetalningar.

Konfidentialitet betyder att information ska hållas konfidentiell vilket innebär att man vill hindra utomstående från att ta del av känslig data. Hemlighetshållande och sekretess är begrepp som ingår i samlingsnamnet konfidentialitet. (Gollman, 2011) Enligt Shon & Swatman (1998) är hemlighållande av privat information en viktig faktor vid all elektronisk handel. Utifrån en konsuments handlingsvanor samt handlingsmönster kan man dra slutsatser om en person och dennes livsstil. Sparas alla köp en person gör under exempelvis ett år så får man en tydlig bild av dennes intressen. Således kan på så sätt en användarens privata liv äventyras om information sparas. Emellertid finns det en tydlig intressemotsättning gällande integritet mellan kunder och exempelvis myndigheter och banker. En kund vill inte bli spårad samtidigt som en bank vill kunna ha insyn i gjorda transaktioner om det finns en misstanke om illegala aktiviteter. (Shon & Swatman, 1998) Detta hör samman med ansvarighet, dvs. att information om transaktion och köp måste sparas och skyddas för att på sätt kunna spåra aktioner som äventyrar säkerheten, samt för att kunna ställa den ansvarige till svars. (Gollman, 2011) Dessutom är det i princip omöjligt att genomföra en transaktion utan att

lämna någon form av personlig information, t.ex. personliga uppgifter som adress eller liknande. (Ackerman, Cranor, & Reagle, 1999)

Integritet handlar om att en utomstående inte ska kunna modifiera känslig information. Integritet och konfidentialitet är starkt sammanvävda, om man definierar integritet som att man vill förhindra att utomstående gör intrång, vilket liknar definitionen av konfidentialitet. (Gollman, 2011) Vidare menar Cleff (2007) att vid mobiltelefonanvändning uppfattas intrång på användarnas integritet som mer påtagligt och allvarligt, än vid användningen av annan teknologi.

Tillgänglighet definieras som att tjänsten ska vara tillgänglig för användaren vid den tidpunkt denne önskar utnyttja den. Exempel på en attack som är ett hot mot tillgängligheten är Denial of Service (Gollman, 2011).

Pålitlighet och säkerhet avser olyckor och attacker som kan drabba ett system och hur man skyddar sig mot dessa. (Gollman, 2011) Vi kommer att närmare gå in på attacker och hot som är relevanta för vårt forskningsområde i kapitel 2.4.

Information om konsumenterna är en viktig aspekt att beakta vid mobilbetalning. Mallat (2007) har i sin kvalitativa studie studerat mottagligheten av mobilbetalningar hos konsumenter. Det finns en oro hos konsumenterna att känsliga uppgifter som t.ex. personlig information och köphistorik sparas. På så sätt skulle deras betalningar och de själva kunna bli spårade: ”…similar to payment cards, the mobile phone will leave traces about where and what you have purchased.. And I already have the feeling that Big Brother is watching.” (Mallat, 2007, s.425)

Vidare så är många konsumenter ovilliga att dela med sig av personlig information, av rädsla för att informationen ska sparas och eventuellt skickas vidare till utomstående utan konsumentens vetskap. Denna rädsla kan ha hindrat spridningen av den elektroniska handeln. (McKnight, Choudhury, & Kacmar, 2002)

2.2 NFC-teknologin

NFC (Near Field Communication) är en vidareutveckling av RFID och är en trådlös kommunikations-teknologi, främst för kommunikation på kort avstånd (proximity). Teknologin tillåter användaren att överföra information på ett avstånd på upp till 10 cm. Fördelarna med NFC jämfört med andra trådlösa kommunikationsformer är att det är enkelt och praktiskt. Med detta menas att transaktioner startar automatiskt, om NFC-enheten är i närheten av en läsare eller en annan NFC-enhet. Teknologin kan implementeras i mobiltelefoner vilket innebär att dessa kan användas som kontaktlösa kreditkort eller kontaktlösa biljetter. (Madlmayr, Langer, Kantner, & Scharinger, 2008)

NFC-enheter använder sig av en magnetisk, induktiv koppling för att sända information från en enhet till en annan, på nära avstånd. En NFC-enhet som har sin egen strömkälla kallas för

aktiv, medan en enhet utan strömkälla är passiv. Vid en koppling absorberar en passiv enhet energi från en aktiv enhet, under förutsättning att avståndet är tillräckligt kort. Detta möjliggör enheterna att kommunicera och utbyta data. (NFC Forum, 2011)

NFC-chipet tillverkas med en antenn och en analog modulator/demodulator som används för att sända och ta emot signaler. Detta integreras på ett silikonchip. Även en radiovågsdetektor integreras för att upptäcka signaler på 13.56MHz. (NFC Forum, 2011)

2.2.1 Användningsområden, möjligheter och fördelar

Användningsområden för NFC delas enligt NFC Forum (2011) in i tre kategorier:

- P2P, där NFC används för att upprätta kommunikation mellan två enheter.
- Betalning (POS) och biljetthantering där NFC kan användas i den framväxande infrastrukturen för biljettbetalningar i till exempel kollektivtrafiken.
- Servicehantering, där NFC används för att upptäcka eller "låsa upp" en annan service, till exempel att öppna en kommunikationslänk för informationsöverföring.

Kredit- och betalkortsföretag, banker och mobiloperatörer ser ett värde i utvecklandet av betalningsapplikationer genom NFC-teknologin och mobiltelefoner. Företagens intresse för teknologin är en av drivkrafterna till utvecklandet av en NFC-standard. För kortföretagen är NFC-betalningar smidigare och mindre kostsamma att hantera i jämförelse med kontanter och andra traditionella betalmedel. Hanteringen innebär också att konsumenten skapar en historik också över transaktioner på mindre summor. Enligt Innovision (2007) kommer teknologin inledningsvis att användas för transaktioner med relativt små summor med låg risk för bedrägeri, så som snabbmat, kiosker, parkeringar och diverse försäljningsautomater.

Vid biljettbetalning idag, köper konsumenten vanligtvis ett plastkort med en förbestämd summa integrerat i kortets chip. När konsumenten använder kortet dras kostnaden från summan och lämnar kortet med en ny balans. När kortet är tomt på pengar kan konsumenten antingen kassera kortet, eller ladda det på nytt. Denna metod har ett antal fördelar gällande användarvänlighet och snabb tillgänglighet, såsom i kollektivtrafiken. En annan fördel är att konsumenten inte behöver inhandla ett kort varje dag. Möjligheten att ladda kortet online eller genom periodvis betalning innebär även ökad effektivitet. Problem med köbildning minskas och det behövs mindre personal. (Nokia, 2007)

Även om metoden ovan fungerar bra är smart cards egentligen inte speciellt smarta, enligt Nokia. Här ser Nokia att NFC kan innebära en förbättring av detta användningsområde. Genom att byta ut kortet mot en NFC-redo mobil kan konsumenten dra nytta av alla fördelarna med kortet, men med ökad funktionalitet genom ett användarinterface. Interfacet skulle t.ex. kunna visa nuvarande balans på kortet eller antal resor kvar. Den aktuella trafiksituationen kan även erhållas genom mobilen. Genom att koppla sitt betalkort till

mobilen ökar man effektiviteten ytterligare genom att behovet av påfyllning försvinner. Nokia menar även att man kan koppla flera betalkort till samma mobil och den kan då betraktas som en virtuell plånbok, med ett antal kort, debet och eller kredit. De flesta användare av mobiler, har den numera alltid med sig. Nokia menar att NFC-mobilen så småningom kommer att leda till att konsumenten inte behöver en traditionell plånbok. Nokia nämner även fler fördelar med NFC-tekniken, men som inte handlar om betalning, så som snabb informationshantering. (Nokia, 2007)

Andra fördelar med teknologin är att teknologin är kompatibel med existerande RFID-strukturer, taggar och kontaktlösa smart cards. Den är även lätt att använda och kräver inga kunskaper om teknologin. Användaren behöver endast starta kommunikationen genom att sammanföra de två enheterna. Dessutom är sändningsavståndet tillräckligt kort för att kommunikationen skall brytas när användaren separerar enheterna. Det korta avståndet bidrar även till ökad säkerhet - finns det ingen annan enhet i närheten pågår det ingen annan kommunikation. (Ok, Coskun, Aydin, & Ozdenizci, 2010)

2.3 NFC i mobila enheter

En mobiltelefon som är NFC-redo har ett NFC-chip installerat. Om NFC-funktionen i telefonen inte är avstängd, är den aktiv och skannar konstant omgivningen för NFC-taggar. När en tag upptäcks talar chipet om för ett NFC-kompatibelt program att taggen finns, och programmet bestämmer sedan vad den skall göra. Om telefonen inte har ett NFC-program eller en applikation för NFC, är det telefonens operativsystem som läser taggen. Om taggen innehåller kompatibel data, förs den över till telefonen och den applikation som skall hantera informationen. (Ok, Coskun, Aydin, & Ozdenizci, 2010)

2.3.1 Betalning med NFC

Mobilbetalning med NFC kan ske genom att den mobila enheten sammankopplas med exempelvis ett kredit- eller debetkort och att NFC-chipet i telefonen sedan kommunicerar med handlaren via POS-systemet. Betalningen kan ske vid bemannade eller obemannade POS-system. För att utföra en betalning för konsumenten telefonen nära den kontaktlösa POS-enheten, och transaktionen går igenom precis som vid en betalning med ett bankkort. (Microsoft, 2009)

En mobilbetalning med NFC kan enligt Microsoft (2009) ske på följande vis: Konsumenten tecknar en betaltjänst med sin bank och en betalning initieras sedan i samband med det aktuella köpet. Innan betalningen kan utföras måste konsumenten godkänna transaktionen. Slutligen genereras ett kvitto till konsumenten och betalningen hamnar i historiken i den mobila enheten.

2.4 NFC – Säkerhet

2.4.1 Analys av hot, risker och attacker

En *risk* är en funktion av *sannolikhet* för att ett *hot* inträffar vilket resulterar i *sårbarheter*. (Dhillon, 2007) Gollman (2011) definierar en risk som hur stor möjligheten är att en attack eller incident kan komma att skada systemet.

Det kan vara svårt skilja på ett hot och en attack: ”A threat materializes when an attack succeeds.” (Gollman, 2011, s. 24) En *attack* mot systemet består av en sekvens av aktioner som utnyttjar svagheter eller sårbarheter i systemet. Detta kan i sin tur negativt påverka en *tillgång*.

För att utvärdera en risk så krävs att man visar på hur allvarlig attacken är (vilka konsekvenser den har), samt sannolikheten för att attacken inträffar. Sannolikheten beror på hur sårbart systemet är, dvs. hur lätt attacken kan genomföras. (Gollman, 2011)

Eftersom NFC-teknologin används vid kontaktlös läsning och identifikation av läsare och enheter, samt att kommunikationen sker ”osynligt” så kan säkerhet och integritet äventyras. Attacker mot en NFC-enhet kan således ske utan att användaren uppfattar det. Dessutom finns det mycket att vinna på att attackera och ta över en NFC-enhet pga. den känsliga information som hanteras, inte minst vid betalningar. (Madlmayr, Langer, Kantner, & Scharinger, 2008)

2.4.2 Tillgångar

En riskanalys inleds med att identifiera tillgångarna, resurserna, i ett system som måste skyddas. Att värdera tillgångar kan vara svårt, särskilt att värdera data och information och dess betydelse för informationsägaren. Information som läcker till någon utomstående kan vara farlig. Gollman (2011) delar in tillgångarna i hårdvara, mjukvara, data och information, samt rykte och anseende. Indelningen kan anses som generell då den gäller alla IT-system.

Applicerat på mobila enheter, vid betalningar med NFC, blir tillgångarna som följer:

- Mobil enhet
- Operativsystem och applikationer
- Känslig information om konsumentens betalningar och köp, t.ex. kortinformation, bankinformation, betalningsmottagare samt köp och betalningshistorik

Naumann & Hogben (2008) har utvecklat indelningen av tillgångarna ytterligare och den är anpassad för säkerhet hos mobila enheter. Känslig information som finns lagrad i den mobila enheten är en tillgång som måste vara skyddad. Känslig information kan vara personlig information, t.ex. namn, födelsedatum och bilder samt inloggningsuppgifter och lösenord. Det kan också röra sig om information om var användaren befinner sig, vilket möjliggör spårning av denne. Detta är ett känsligt område då användaren vill ha total kontroll över vem som har

information om var han eller hon befinner sig (He, Wu, & Khosla, 2004). Tillgång till bankkonton och pengar är en annan tillgång. Om en attackerare på något sätt, exempelvis genom phishing, får tillgång till användarens bankkonto finns det risk för att pengar blir överförda utan användarens vetskap. Tillgången till tjänsten, t.ex. en betalning, och huruvida den är tillgänglig eller inte, ses även som en resurs. Slutligen kan tillgång till byggnader och privata ägodelar även de räknas som tillgångar. (Naumann & Hogben, 2008)

2.4.3 Hot och attacker mot mobiltelefoner med NFC

Attackmetoder mot NFC-mobilbetalningar kräver ett brett fält av expertis kring fysik, informatik och kryptografi. Eftersom applicerandet av kunskapen om dessa områden för användande vid attacker är väldigt komplext, har företag svårt att försäkra sig om god säkerhet rörande NFC och mobilbetalningar. (Pasquet, Reynaud, & Rosenberger, 2008)

Nedan presenterar vi en sammanställning av de hot som oftast nämns i litteraturen och därför är mest intressanta för vårt arbete.

Tjuvlyssning
Eftersom NFC är en trådlös kommunikationsform så finns naturligtvis risken att en utomstående person kan "tjuvlyssna". NFC använder sig av radiovågor för att skicka information och således kan en utomstående med hjälp av en antenn ta emot de skickade signalerna. Med rätt kunskap kan även informationen i radiovågorna extraheras och tolkas. Med det faktum att NFC verkar på korta avstånd och därför endast kräver lite ström för att enheter skall kunna kommunicera med varandra, är svårt för en utomstående att tjuvlyssna på kommunikationen. Det finns ett par parametrar som avgör hur långt ifrån enheterna personen som utför attacken behöver vara för att lyckas. Kvaliteten på antennen och mottagaren och hur dessa är konstruerade är av stor vikt. Eventuella blockader så som väggar, metall eller störningar av andra slag har även påverkan. Eftersom faktorerna är många är det svårt att fastslå det exakta avståndet som krävs för en lyckad attack och det blir således svårt att fastslå riktlinjer för säkerhet. (Haselsteiner & Breitfuß, 2006)

NFC kan inte på egen hand skydda mot tjuvlyssning, men det kan noteras att data som sänds i passive mode är svårare att tjuvlyssna. Att använda sig av passive mode är dock förmodligen inte tillräckligt för de flesta applikationer som sänder ut känslig data. Ett alternativ är att upprätta en säker kanal mellan två NFC-enheter med hjälp av ett standardiserat krypteringsprotokoll. (Haselsteiner & Breitfuß, 2006)

Datakorruption, datamodifikation och införande av data
Det också möjligt för en utomstående att istället för att enbart lyssna till en signal, även modifiera den information som skickas. Vid datamodifikation manipuleras data och mottagaren tar således emot manipulerad data. Detta kan möjliggöras genom att denne tredje part skickar frekvenser vid rätt tidpunkter. (Haselsteiner & Breitfuß, 2006)

En form av modifikation eller korruption av data, är en så kallad DoS-attack, där någon stör kommunikationen mellan två parter. Attackeraren manipulerar inte data som överförs utan stör själva signalen. En DoS-attack sker vid sammanförandet av en NFC-enhet och en tag, även en informationslös sådan, vilket orsakar en reaktion i enheten. Även om det endast är ett felmeddelande som skapas är detta ett sätt att hålla enheten upptagen. Denna attack kan utföras om attackeraren har god förståelse för kodningen och timingen för signalen. (Madlmayr, Langer, Kantner, & Scharinger, 2008). För att sammanfatta dessa attacker använder vi oss av begreppet *störning*.

Vid införande av data sänder den som utför attacken meddelanden när ett utbyte av data äger rum. Om attacken utförs korrekt så kan personen ”komma före” den ursprungliga sändaren och således skicka sin information till mottagaren. Den här metoden lyckas endast om svarsenheten behöver relativt lång tid på sig för att svara. Om insatt data överlappas med korrekt data blir informationen istället korrupt. (Haselsteiner & Breitfuß, 2006)

NFC-enheter kan skydda sig mot datakorruption och modifikation genom att undersöka radiovågsfältet när data skickas och på så sätt upptäcka eventuella attacker. Kraften som behövs för att genomföra dessa former av attacker är alltid tillräcklig för att NFC-enheterna skall kunna upptäcka dem. Genom att använda sig av aktivt läge, blir det omöjligt för attackeraren att modifiera data, men enheterna blir då istället sårbara mot tjuvlyssning. Det mest lämpliga alternativet är det förstnämnda, där den utsändande NFC-enheten kontinuerligt undersöker radiovågorna och avslutar sändningen vid en eventuell attack. (Haselsteiner & Breitfuß, 2006)

Det finns tre möjliga motåtgärder mot införande av data. Om den svarande enheten svarar utan fördröjning kan attackeraren inte vara snabbare än den riktiga enheten. Attackeraren kan vara lika snabb som den korrekta enheten men i det fallet svarar enheterna samtidigt och data blir istället korrupt. Den andra möjligheten innebär att avlyssna den svarande enheten när överföringen startar och på så sätt upptäcka om någon försöker föra in annan information. Det tredje alternativet är, som nämndes tidigare att upprätta en säker kanal mellan enheterna genom kryptering som ett skydd mot avlyssning. (Haselsteiner & Breitfuß, 2006)

Man-in-the-Middle

I en Man-in-the-middle-attack lurar en tredje part två parter att kommunicera med varandra. Informationen som skickas mellan de två parterna går då även till denna tredje part. De två parterna har ingen uppfattning om att de inte skickar och tar emot data till och från varandra. Om attackeraren är tillräckligt nära kommunikationen är det möjligt för denne att tjuvlyssna på data som sänds. En sådan attack är dock mycket svår att genomföra i praktiken då det är relativt enkelt för de riktiga parterna att upptäcka om en tredje part är inblandad i kommunikationen. (Haselsteiner & Breitfuß, 2006)

Som nämnt ovan är det i princip omöjligt att utföra en Man-in-the-middle-attack och rekommendationen är att använda sig av passivt läge där överföringen genereras konstant av en av de verkliga enheterna. Den aktiva enheten borde genom att lyssna på överföringen

säkerhetsställa att det inte förekommer störningar från en eventuell attack. (Haselsteiner & Breitfuß, 2006)

Spårning
NFC-enheter har unika identifikationsnummer som skickas för att inleda kommunikation med t.ex. en läsare. När användaren befinner sig i närheten av en NFC-läsare kan systemet spara det unika id:et i en databas. Detta innebär att användarens rörelsemönster kan kartläggas och spåras. (Naumann & Hogben, 2008)

Vidare finns det andra hot som faller under vår indelning eller kan ses som generella hot som inte är exklusiva för NFC, som t.ex. nätfiske, relä-attack, fysisk attack och stöld eller förlust. (Madlmayr, Langer, Kantner, & Scharinger, 2008; Naumann & Hogben, 2008)

3 Metod

I detta kapitel presenterar vi den metod vi har använt för vårt arbete. Inledningsvis beskrivs hur undersökningen genomförts. Sedan följer en redogörelse för hur vi utformat enkäten och hur den har distribuerats. Analysmetoden gås därefter igenom. Slutligen diskuteras etik och forskningskvalitet samt källkritik.

3.1 Genomförande

En litteraturgenomgång är första steget i vårt arbete. Syftet med denna genomgång är att skapa en kunskapsgrund och beskriva relevanta definitioner för det fortsatta arbetet. Majoriteten av den litteratur vi har använt består främst av akademiska artiklar, men även annan vetenskaplig litteratur i form av böcker. Majoriteten av artiklarna är hämtade från Lunds universitets databas LibHub, men en del har vi sökt fram genom Googles sökmotor.

Efter att vi byggt kunskapsgrunden drog vi slutsatsen att en enkät borde vara den mest optimala metoden för datainsamling. Valet grundades på några av de fördelar som Ejltertsson (2005) beskriver. Bland fördelarna fann vi att respondenten i lugn och ro har möjlighet att begrunda frågorna och överväga svarsalternativen, vilket är fördelaktigt då vi ser de eventuella frågorna som relativt svåra att begripa utan eftertanke. Valet av en kvantitativ ansats grundar sig även på att metoden är mest lämplig vid beskrivningen av ett fenomens frekvens eller omfattning. (Jacobsen, 2002)

Genom att distribuera enkäten via datorn och internet, sparas tid och pengar i jämförelse med andra distributionsformer. Andra fördelar med internet som distributionskanal är att man når ut till ett stort antal människor och kan samla in data relativt snabbt. (Ejlertsson, 2005)

Efter insamlandet av empiri, analyserades resultatet och jämfördes med vår teoribas. Utifrån denna analys och jämförelse för vi sedan ett resonemang om vår forskningsfråga. Därefter drar vi de för denna undersökning relevanta slutsatserna.

3.2 Enkätutformning

3.2.1 Urval

Vid enkätundersökningar är stickprov ur populationen det vanligaste sättet att göra urval. Stickprovet skall spegla populationen genom en miniatyr. (Ejlertsson, 2005) Vi delade ut enkäten till ca 500 vänner och bekanta, genom sociala medier och e-mail. Enkäten var tillgänglig för alla som hade tillgång till länkadressen, och vi kunde därför inte kontrollera vem som svarade på enkäten.

3.2.2 Enkäten och dess utformning

Enkäten utformades och distribuerades med hjälp av Google Spreadsheet. Enkäten var anonym och de svarande fick ingen kompensation för sitt deltagande.

Enkäten består av 19 frågor. Frågorna är både öppna och slutna, d.v.s. vi har till största del använt slutna frågor med fasta svarsalternativ och ett fåtal där de svarande ombeds motivera sina svar. Bortsett från bakgrundsfrågorna, frågor med endast ja och nej som svar och de som kräver motivering, så har vi valt att använda påståenden. Enligt (Jacobsen, 2002) är påståenden en mycket vanlig form av frågor vid mätning av känslor och åsikter, och det är denna teori vårt val av frågeform grundar sig i.

I bilaga A finns motiveringar för enkätfrågorna och hur de är kopplade till teorin.

3.3 Etik och forskningskvalitet

3.3.1 Validitet och reliabilitet

Som Jacobsen (2002) förklarar innebär validitet att insamlad data måste vara giltig och relevant. För att ha en så hög begreppsvaliditet som möjligt har enkätfrågorna i högsta möjliga grad förankrats i den teoretiska kunskapsbasen, vilket även går i linje med Ejlertsson (2005). Att undersöka användarnas syn på säkerhet kan ses som en tämligen komplex process. Användarnas säkerhetsmedvetenhet består av flera element, således har vi använt många frågor. Många frågor underlättar en undersökning och mätning av fenomenet (Jacobsen, 2002).

Med reliabilitet avses huruvida upprepade mätningar ger samma resultat. För att försöka få så hög reliabilitet som möjligt var vi noggranna med att utforma enkätfrågorna på ett korrekt sätt, dvs. att de var tydliga och välformulerade (Ejlertsson 2005). Vi lät fem personer testa enkäten och komma med åsikter på frågornas formuleringar.

3.3.2 Etik

Enligt Jacobsen (2002) bör man eftersträva diskretion och att de personer som deltar i undersökningen förblir anonyma. Eftersom enkäten är anonym, dvs. inget namn behöver anges, samt att endast frågor om kön och ålder förekommer, kan inte svaren kopplas till en specifik person. Vidare är det ett stort antal svarande vilket ytterligare ökar anonymiteten.

Vi klargjorde syftet med enkäten i inledningen för att informera de svarande om vad den handlade om och varför de skulle delta. Dessutom försökte vi vara tydliga med hur frågorna formulerades för att de som deltog i enkäten verkligen skulle förstå vad de svarade på. (Jacobsen, 2002)

3.3.3 Kritik av metoden

Det finns ett antal metoder för att förvissa sig om att reliabiliteten är hög (Ejlertsson, 2005). Ingen sådan kontroll genomfördes och således kan inte en hög reliabilitet bevisas.

Ejlertsson (2005) beskriver generella nackdelar med enkätundersökningar, vilka bör begrundas. Det finns inget utrymme för den svarande att ställa kompletterande frågor kring t.ex. otydlig information i enkäten. Dessutom kan åsikter uppfattas som påtvingade vid de standardiserade frågor och svarsalternativ som förekommer i en enkät. (Jacobsen, 2002)

Vi är även medvetna om att det föreligger ett bekvämlighetsurval av respondenter i vår undersökning. Detta beror på att urvalet främst är vänner och bekanta i vår egen åldersgrupp. Enligt (Jacobsen, 2002) ger bekvämlighetsurval några fördelar: vi undgår kostnader och vinner tid i samband med urvalet, då vi väljer dem som vi på enklast väg har möjlighet att kontakta. Metoden har alltså en del svagheter, men vi anser att tillräcklig empiri har samlats in för att göra studien valid. Vi är medvetna om att studien har ett relativt stort bortfall, men vi kan inte analysera detta bortfall närmare då det föreligger ett s.k. bekvämlighetsurval, vilket enligt Jacobsen (2002) omöjliggör en sådan analys.

Vi vill dessutom understryka att resultatet och tillhörande slutsatser baseras på ett tämligen begränsat åldersintervall, närmare bestämt personer mellan 18 och 35 år. Detta skulle kunna ses som något som påverkar validiteten i vår studie negativt. Denna möjligen snäva åldersinledning rättfärdigas emellertid av vår hypotes om ålder och vår inledande avgränsning.

4 Empiri

I detta kapitel redovisas vår insamlade empiri från enkäten. Endast data presenteras och inget resonemang eller analys genomförs. Analysen introduceras först i kapitel 5. Empirin presenteras i form av stående och liggande stapeldiagram, och på frågor med endast två svarsalternativ visas resultatet med hjälp av cirkeldiagram. Vi har också använt oss av tabeller för att visa medel-, median- och modalvärde för rangordnade svar, för att kunna ge en tydlig överblick.

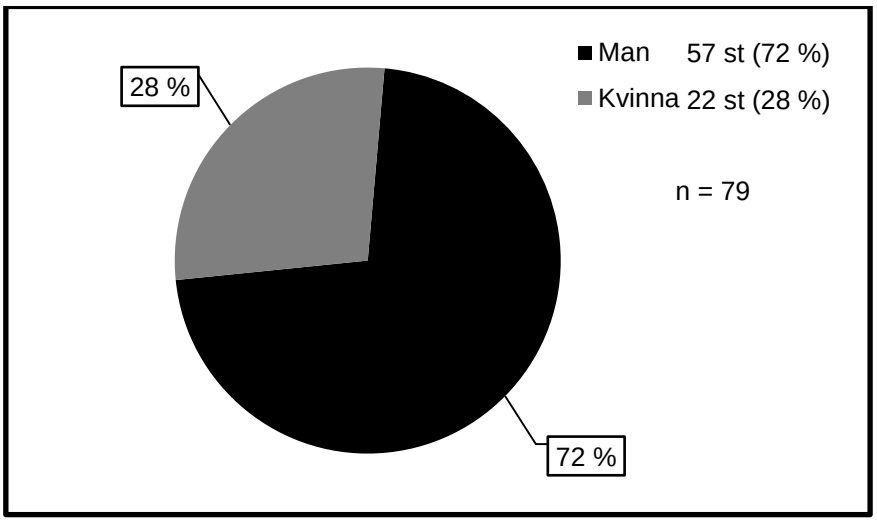
4.1 Deltagande

Enkäten delades ut till ca 500 personer via sociala medier och email. Totalt svarade 79 personer på enkäten och urvalet bestod främst av familj, vänner och bekanta. Av de svarande bestod 72 % av män och 28 % av kvinnor och den huvudsakliga åldersgruppen (95 %) var mellan 18-35 år. Enkäten fanns tillgänglig mellan 4/5-9/5, 2011.

4.2 Redovisning av empiri

Här följer en redovisning av de inkomna svaren från enkäten.

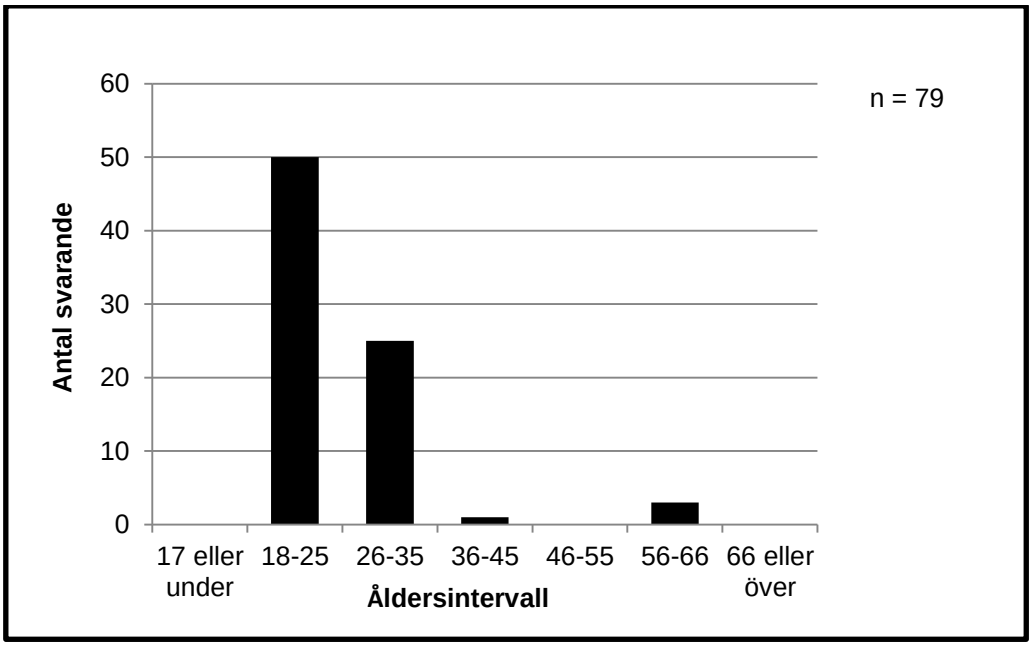
Fråga 1 - Kön



Figur 4.1 Enkätsvar - Fråga 1

Majoriteten, cirka tre fjärdedelar (72 %) av de svarande är män. (Figur 4.1)

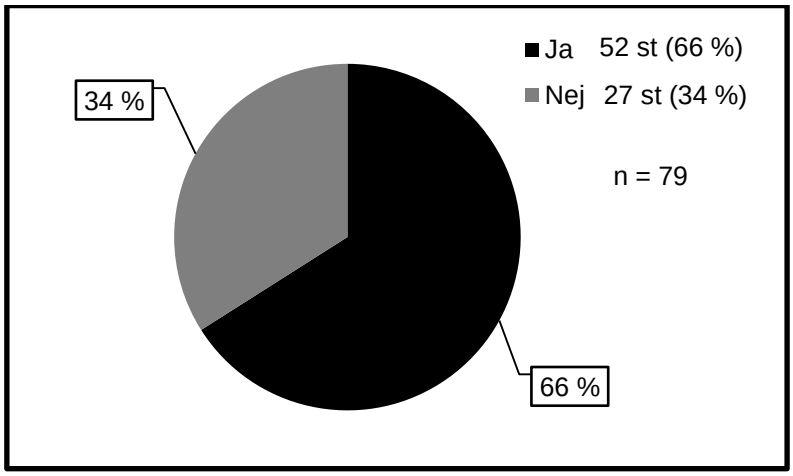
Fråga 2 – Ålder



Figur 4.2 Enkätsvar - Fråga 2

Resultatet visar (Figur 4.2) att ungefär 63 % av svaren kommer från personer mellan 18 och 25 år och 32 % är mellan 26 och 35 år. Ingen svarande är under 17, eller över 66 år. Där finns heller inget svar från någon mellan 46 och 55 år. I åldersgruppen 36-45 finns det endast en svarande.

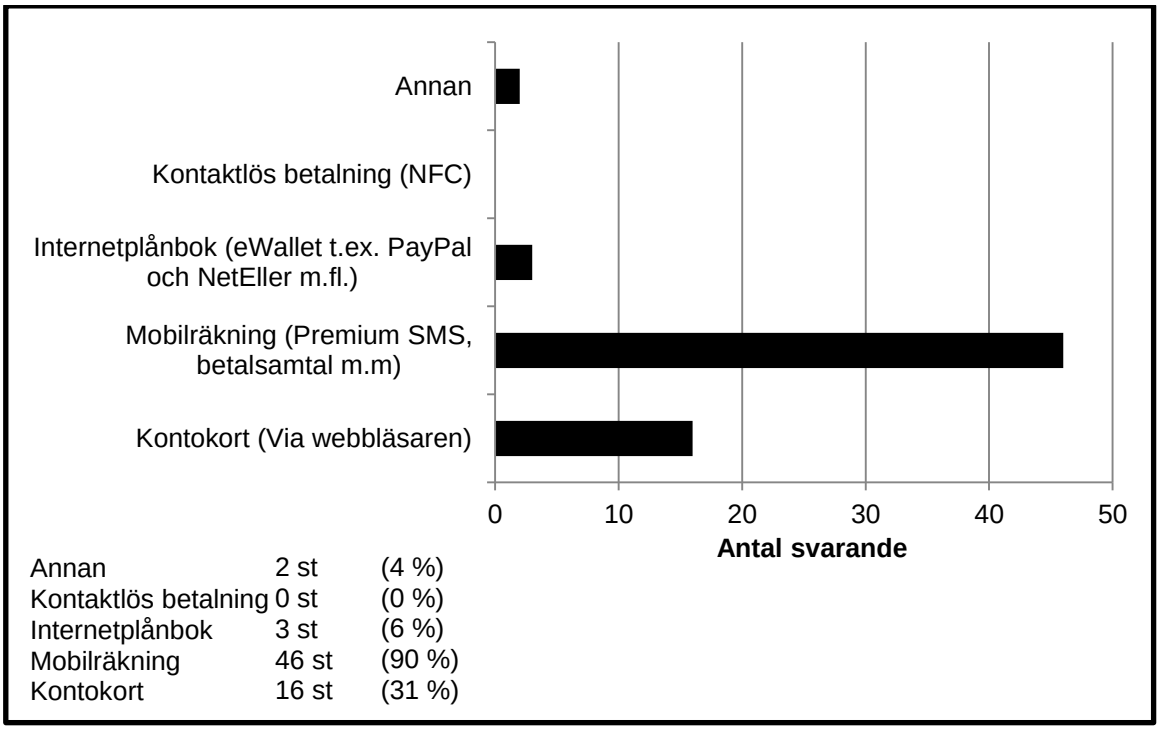
Fråga 3 – Har du någonsin betalat med din mobiltelefon?



Figur 4.3 Enkätsvar - Fråga 3

Majoriteten (66 %) av de svarande har någon gång betalat med sin mobiltelefon. (Figur 4.3)

Fråga 4 – Om ”Ja”: Vilken metod använde du för att betala?



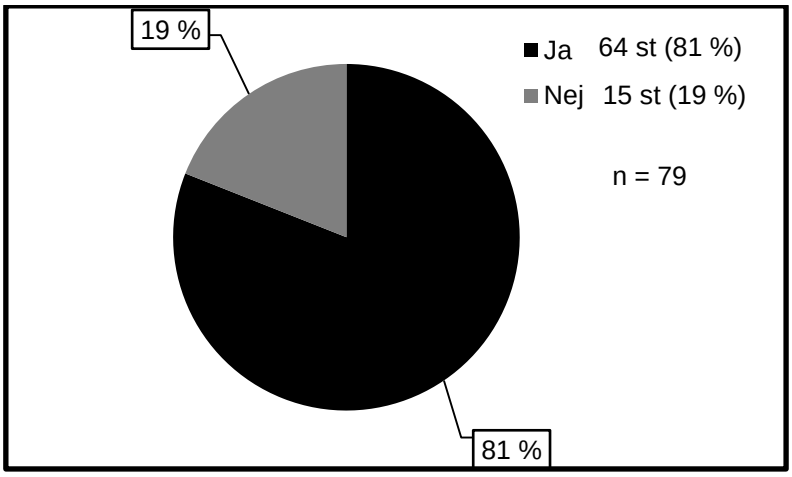
Figur 4.4 Enkätsvar - Fråga 4

Figur 4.4 visar att 56 personer någon har gång betalat med en mobiltelefon och i störst utsträckning (90 %) har utfört dessa betalningar via en mobilräkning. Ungefär var tredje svarande (31 %) har betalat via webbläsaren. 6 % har betalat med internetplånbok medan ingen av de svarande har betalat kontaktlöst med NFC. Två personer har uppgivit att de betalat genom ”iTunes” samt ”hemskickad faktura” i övrigt-rutan. Alla svarsmotiveringar återfinns i Bilaga C.

Fråga 5 – Om du svarade ”Nej” på föregående fråga: var vänlig motivera varför

23 svarande har aldrig betalat med en mobiltelefon och 14 av dessa (61 %) motiverar detta med att de aldrig fått tillfället eller haft ett behov av att betala med mobiltelefonen, bl.a. för att de redan betalar med sin dator. Fyra personer uppger att anledning till att de aldrig betalat med en mobiltelefon är av teknisk karaktär, såsom föråldrad mobiltelefon eller misslyckade försök till betalning. Tre personer uppger säkerhetsaspekten som skäl till att de aldrig betalat med en mobiltelefon. Alla svarsmotiveringar återfinns i Bilaga C.

Fråga 6 – Är du intresserad av att betala med mobiltelefonen i framtiden?



Figur 4.5 Enkätsvar - Fråga 6

Cirkeldiagrammet (Figur 4.5) visar att en majoritet (81 %) är positiva till att betala med en mobiltelefon i framtiden.

Fråga 7 – Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från ”Minst viktig” till ”Viktigast”.

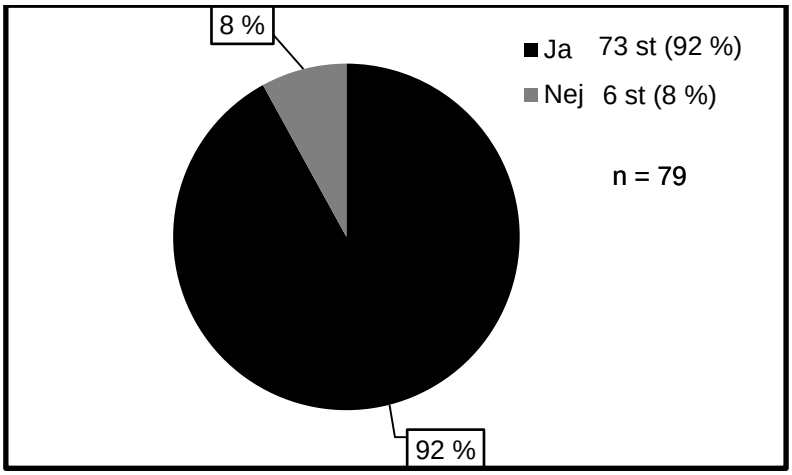
Svaren är rangordnade på en skala från 1 till 5, där 1 är ”Minst viktig” och 5 är ”Viktigast”.

Tabell 4.1 Enkätsvar – Faktorer för mobilbetalning

Faktor	**Medelvärde**	**Median**	**Modalvärde (% av svar)**
Användarvänlighet	3,68	4	4 (35 %)
Pålitlighet och säkerhet	4,66	5	5 (77 %)
Användbarhet	3,48	4	4 (32 %)
Kostnad	3,44	4	4 (34 %)
Kompabilitet	2,86	3	1 (30 %)

Resultatet i tabellen (Tabell 4.1) visar att användarna anser att pålitlighet och säkerhet är den viktigaste faktorn vid mobilbetalningar. Hela 77 % anser säkerhet som ”viktigast” av de ovan nämna faktorerna. Faktorerna användarvänlighet, användbarhet och kostnad anses ungefär lika viktiga, med ett medelvärde på runt 3,50. Kompabilitet är enligt användarna minst viktigt, vilket bl.a. det låga modalvärdet visar på.

Fråga 8 – Hade du kunnat tänka dig att betala ”kontaktlöst” med din mobiltelefon?



Figur 4.6 Enkätsvar - Fråga 8

Drygt nio av tio (92 %) av de svarande är intresserade av att betala kontaktlöst med sin mobiltelefon. (Figur 4.6)

Fråga 9 - Om du svarade "Nej" på föregående fråga, var vänlig motivera varför. Vill du lämna en kommentar till Ja-svaret går det också bra.

Sammanlagt är det 13 st. som har motiverat sitt svar, vilket både består av det antal som svarade ”Nej” på föregående fråga (6 st.), samt ytterligare 7 personer som har svarat ”Ja” på fråga 8.

8 av 13 (62 %) svarande har angivit säkerhetsaspekten som huvudskälet till varför de är tveksamma till att betala kontaktlöst. Alla svarsmotiveringar återfinns i Bilaga C.

Fråga 10, 12, 14, 16 – Jag anser det troligt att följande hot inträffar

Frågorna behandlar hur troligt användarna anser att hoten inträffar på en skala från 1 till 5, där 1 är ”instämmer inte alls” och 5 är ”instämmer helt”.

Tabell 4.2 Enkätsvar – Hot & trolighet

Hot	**Medelvärde**	**Median**	**Modalvärde (% av svar)**
Tjuvlyssning	2,92	3	4 (32 %)
Störning	2,23	2	1 (38 %)
Spårning	3,96	4	5 (44 %)
Lagring av information	4,09	4	5 (41 %)

Spårning och lagring av information anses av användarna som troliga hot och drygt 40 % av de svarande ”instämmer helt” med att dessa kan inträffa vid en kontaktlös betalning. Att en utomstående stör kommunikationen anses dock som mindre eller inte alls troligt. (Tabell 4.2)

Fråga 11, 13, 15, 17 – Jag anser dessa hot vara:

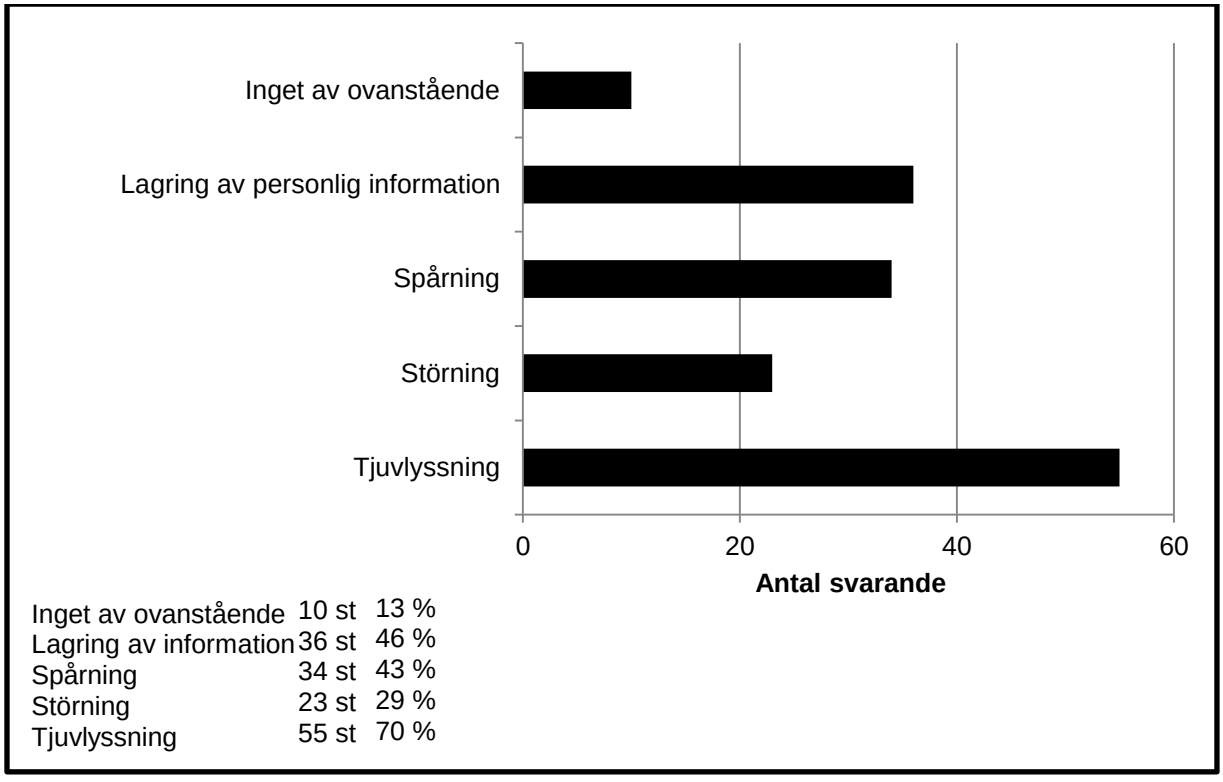
Frågorna behandlar hur användarna värderar hoten efter hur allvarliga de anses vara. Värdering sker på en skala från 1 till 5, där 1 är ”inte särskilt allvarligt” och 5 är ”mycket allvarligt”.

Tjuvlyssning anses av de svarande som det mest allvarliga hotet, med ett medelvärde på ca 4 och med 43 % som tycker att det är ”mycket allvarligt”. Lagring av information har ett lägre medelvärde och median, samtidigt som nästan en tredjedel av de svarande anser även detta hot som ”mycket allvarligt”. Störning och spårning är enligt användarna något mindre allvarligt än ovan nämnda hot. (Tabell 4.3)

Tabell 4.3 Enkätsvar – Värdering av hot

Hot	**Medelvärde**	**Median**	**Modalvärde (% av svar)**
Tjuvlyssning	3,95	4	5 (43 %)
Störning	2,94	3	3 (25 %)
Spårning	3,35	3	3 (33 %)
Lagring av information	3,41	3	5 (29 %)

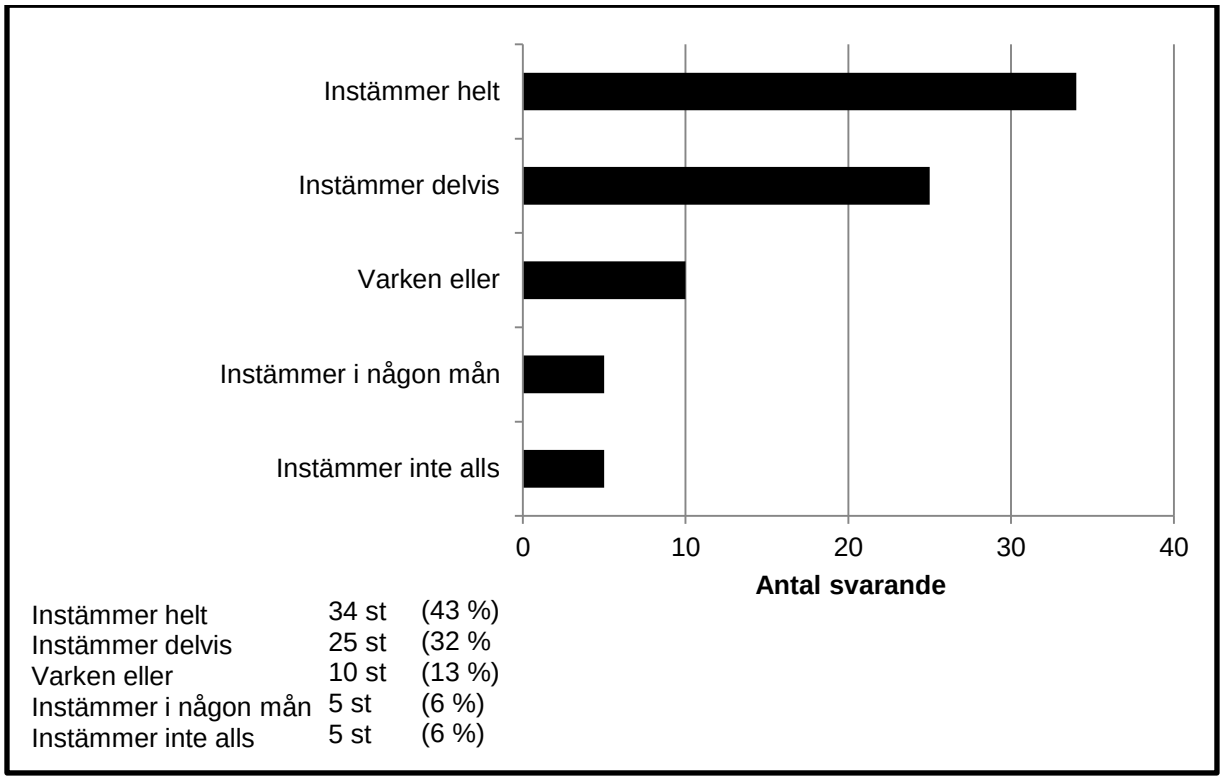
Fråga 18 – Vilket/vilka hot skulle hindra dig från att vilja betala kontaktlöst med din mobiltelefon?



Figur 4.7 Enkätsvar - Fråga 18

Tjuvlyssning är det hot som flest svarande (70 %) anser vara det största hotet för att hindra dem från att betala kontaktlöst. Spårning och lagring av information tycker närmare hälften av de svarande är hot som skulle vara hinder. Endast 13 % anser ingen av hoten som hinder för deras användande av kontaktlös betalning. (Figur 4.7)

Fråga 19 – Om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan jag INTE tänka mig att använda det



Figur 4.8 Enkätsvar - Fråga 19

75 % av de tillfrågade instämmer helt eller delvis med att om kontaktlös betalning är mindre säkert än det traditionella användandet av kreditkortet skulle de inte kunna tänka sig att använda det. De resterande tillfrågade har ingen åsikt, instämmer i någon mån eller inte alls. (Figur 4.8)

5 Analys och diskussion

I följande kapitel analyseras och diskuteras resultatet av enkätsvaren. Analysen delas in i två avsnitt för att göra det tydligare för läsaren. Det första avsnittet behandlar användarnas syn på mobilbetalningar. Nästkommande del redogör för användarnas säkerhetsmedvetenhet vid kontaktlösa mobilbetalningar.

5.1 Användarnas syn på mobilbetalningar

Majoriteten (66 %) av de svarande har någon gång betalat med sin mobiltelefon. Det visar att folk är villiga att betala med sin mobiltelefon.

Enligt resultatet har nio av tio betalat via mobilräkning, vilket stämmer överens med tidigare forskning vilket visat att sms-betalningar är det vanligaste betalningssättet för mobilbetalningar i Europa (kap 2.1.1). Ingen av de svarande har använt NFC för att betala kontaktlöst, vilket vi ser som föga förvånande, då det ännu inte finns en standard för detta i Sverige. Trots detta visar empirin, något överraskande, att drygt nio av tio är intresserade av att betala kontaktlöst med mobilen i framtiden. Vi beskrev kontaktlös betalning som användandet av JoJo-korten i kollektivtrafiken, vilket är kontantlöst och kan upplevas som ett smidigt sätt att genomföra en betalning. Dessa faktorer kan ha bidragit till att så många ställde sig positiva till en teknologi de inte har använt och förmodligen har begränsad kunskap om.

Av de svarande som inte har betalat med mobiltelefonen visar resultatet att majoriteten inte haft något egentligt behov av detta (kap 4, fråga 5). Vi ser det som självklart att det måste finnas ett behov hos användaren innan denne kan ta ställning till andra aspekter, så som säkerhet. Därför är det inte förvånande att endast ett fåtal angett säkerhet som anledningen till deras tveksamhet.

Enligt vår enkät är fyra av fem av de svarande positiva till att betala med sin mobiltelefon i framtiden. Detta stärker uppfattningen att mobiltelefonen verkligen är ett framtida betalningsmedel, och att vi är på väg mot det kontantlösa samhället. (kap 2.1)

5.2 Användarnas säkerhetsmedvetenhet vid kontaktlös mobilbetalning

Det finns ett flertal faktorer gällande användaracceptans av ny teknologi, i enkäten nämnde vi de fem viktigaste vid mobilbetalning. Resultatet visar att pålitlighet och säkerhet är den absolut viktigaste faktorn; 77 % av de svarande ansåg denna som mycket viktig. Detta överensstämmer med tidigare studier som visat att säkerhet, tillförlitlighet och integritet är de viktigaste aspekterna att beakta vid mobilbetalningar (kap 2.1.3). Något förvånande är att fler är intresserade av kontaktlös mobilbetalning, än mobilbetalning i stort. Detta beror möjligen

på hur vi presenterade frågan om kontaktlös betalning, där vi liknande det vid JoJo-kort i kollektivtrafiken. En positiv syn på JoJo-kort hos de svarande kan ha påverkat resultatet. Det fanns dock de som var tveksamma och bland dessa var säkerhetsaspekten huvudskälet.

Vår forskningsfråga handlar till stor del om användarnas syn på säkerhet skulle kunna hindra NFC-baserade mobilbetalningar och ökningen av dessa. Eftersom kundernas brist på förtroende kan hindra en sådan ökning (kap 2.1.3), samtidigt som vår empiri visar användarnas fokus på säkerhet, kan man dra slutsatsen att säkerhetsfrågan är den allra viktigaste om NFC och mobilbetalningar ska kunna slå igenom.

Fyra av fem svarande anser att det är mer eller mindre troligt att en utomstående skulle tjuvlyssna på kommunikationen vid en kontantlös betalning. Eftersom svaren är relativt jämnt spridda över hela skalan kan detta tolkas som att de svarandes åsikter skiljer sig mycket från varandra, och att det således finns en osäkerhet gällande hur troliga sådana hot är. Som teorin (kap 2.4.3) visar är det svårt att fastslå hur sannolikt det är att tjuvlyssning inträffar och kan bli ett problem i framtiden. Detta pga. att det är många små faktorer som spelar in.

Något färre än hälften anser tjuvlyssning som något mycket allvarligt. En anledning till detta kan vara att konsumenter är oroliga för att känslig information kommer i orätta händer. Känslig information kan vara diverse inloggningsuppgifter, bankinformation, fakta om var användaren befinner sig samt namn och persondata (kap 2.4.2). Det kan också röra sig om rena integritetsskäl, d.v.s. konsumenters ovilja att dela med sig av information oavsett vad den kan tänkas användas till. Integritet en av de delar som ligger till störst vikt hos konsumenten, dessutom finns även en rädsla att informationen skickas vidare till tredje part utan konsumentens vetskap (kap 2.1.3).

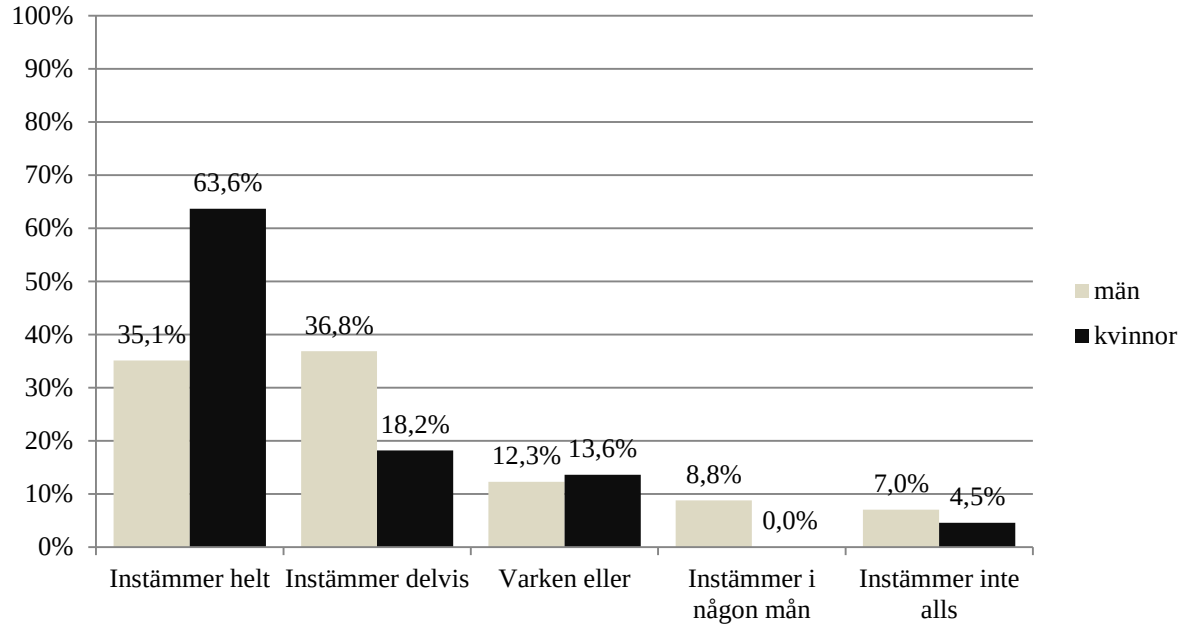
Att information lagras när ett kontaktlöst köp genomförs anser en klar majoritet vara troligt, emellertid råder det delade meningar om lagring av information är allvarligt eller ej. Precis som vi nämnde (kap 2.1.3) är det i princip omöjligt att genomföra en transaktion utan att lämna någon form av personlig information. Användare är i stor grad medvetna om att känslig information som t.ex. personliga uppgifter och betalningsinformation sparas när en konsument slutför ett köp, men det finns en viss acceptans för detta så länge informationen inte hamnar i orätta händer.

Fler än var tredje svarande anser inte att störning är en trolig attack vilket kan bero på att det inte finns någon direkt ekonomisk fördel för någon att utföra detta mot en enskild konsument. Störning kan liknas vid sabotage och kan således uppfattas som ett irritationsmoment mer än ett konkret hot. Av samma anledning har de svarande svårt att se allvaret i en sådan attack. Vidare riskerar inte konsumenten några direkta ekonomiska förluster. Enligt empirin ser de svarande störning som det minst allvarliga hotet.

En klar majoritet anser det troligt att de kan bli spårade när de genomför en betalning med NFC. Vidare anser de svarande att spårning är relativt allvarligt. Anledningen till detta är sannolikt att användare vill lämna så lite information som möjligt om var de befinner sig när de använder sin mobiltelefon. Detta för att ha kontroll över vem som har information om var

de befinner sig (kap 2.4.2). Dessutom kan deras inställning förklaras med att integritet är en särskilt viktigt aspekt vid mobilbetalningar (kap 2.3.1).

Användarnas syn på hoten kan *sammanfattas* med att tjuvlyssning anses vara det hot som till störst grad skulle hindra dem från att betala kontaktlöst i framtiden. Endast ett fåtal svarande anser inte att något av hoten skulle utgöra ett hinder. Vidare visar empirin att en klar majoritet kräver att tekniken ska vara mer säkert än användandet av dagens kreditkort för att användarna ska vilja nyttja NFC som betalningsmedel. Av detta drar vi slutsatsen att användarna ser allvarligt på säkerhetshot vid mobilbetalningar och den generella säkerheten är en viktig aspekt, vilket också vår litteraturgenomgång stödjer (kap 2.3.1).



Figur 5.1 Enkätsvar - Fråga 19 med könsindelning

Vid analysen var det svårt att urskilja tendenser mellan könen på de olika frågorna. Vi finner dock att kvinnor anser säkerhet som något viktigare när vi samkörde fråga 19, *Om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan jag INTE tänka mig att använda det,* med de svarandes kön. Enligt teorin (kap 2.1.2) råder det delade meningar om huruvida olika kön påverkar användarnas vilja att acceptera ny teknologi. I detta sammanhang pekar man gärna på den forskning som visar att män generellt är mer riskbenägna än kvinnor. En klar majoritet av de svarande kvinnorna instämmer helt med påståendet att om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan dessa *inte* tänka sig att använda det, vilket Figur 5.1 visar. Slutsatsen som kan dras av detta är att säkerhet är viktigare för kvinnor, åtminstone i detta avseende.

6 Slutsats

Syftet med rapporten är att besvara vår forskningsfråga om hur medvetna användarna är om säkerheten vid mobilbetalningar. I vår litteraturgenomgång behandlade vi begreppet mobilbetalning samt olika metoder för detta. NFC-teknologin ses som den mest aktuella tekniken för mobilbetalningar i framtiden, således har denna teknologi legat i fokus i rapporten. Det teoretiska ramverket TAM bekräftade säkerheten som den viktigaste aspekten beträffande användaracceptans. Vi har vidare kartlagt de hot och attacker som är troligast att förekomma vid en betalning med NFC.

Med teorin som grund konstruerades en enkät för att få kunskap om hur användarna ser på säkerheten hos NFC. Resultatet av empirin speglade till stor del teorin inom området, dvs. enkätsvaren bekräftade redan förda resonemang från litteraturgenomgången. Genom empirin kan vi dra slutsatsen att användarna är mycket positiva till en framtida betalningslösning med NFC. Samtidigt som användarna ställer sig positiva till mobilbetalningar i framtiden, är det viktigt att beakta säkerheten och integriteten vid användning av teknologin. Teorin och empirin stämmer väl överens och talar för att säkerheten är av yttersta vikt för användarna. Omvänt innebär detta att säkerheten skulle kunna utgöra ett stort hinder för framtida spridning av NFC-teknologin.

Många av hoten mot NFC är direkt kopplade till integritet- och sekretessaspekter gällande information. Användarna är medvetna om att information sparas vid en betalning, samtidigt föreligger det delade meningar om hur allvarligt detta är. En slutsats av detta blir att det finns en acceptans av att information lagras så länge information inte hamnar i orätta händer. Fler slutsatser kan dras om integritetsaspekten. Ett flertal av de som svarat på enkäten framhåller att risken för spårning föreligger, och är allvarlig. Eftersom spårning kan likställas med lagring av information, visar dessa slutsatser att användarna saknar tillit till att deras privata sfär och integritet bibehålls. Att bli avlyssnad ser användarna som ett allvarligt hot, vilket bekräftar teorin om att integritet, som är starkt sammankopplad med säkerhet, är viktigt för att användarna ska känna sig bekväma med teknologin.

Vår forskningsfråga är: *Hur medvetna är användarna om säkerhetsrisker inom mobilbetalning med NFC? Hur värderar användarna dessa risker?*

Ett summerat svar på denna fråga är att användarnas säkerhetsmedvetenhet är hög inom mobilbetalningar och hoten värderas som allvarliga, särskilt när den personliga integriteten står på spel.

Detta leder fram till svaret på vår följdfråga: *Kan säkerhetsaspekten vara ett hinder för NFC-teknologins framtida utveckling och spridning?*

Vi har funnit att användarnas attityd till säkerhet- och integritetsfrågorna, tillsammans med deras brist på förtroende för NFC kan betraktas som ett verkligt potentiellt hinder för ett ökat

användande av denna teknologi. För den framtida utvecklingen och spridningen av denna teknologi framstår således lösningen av dessa frågor som helt avgörande.

6.1 Vidare forskning

Då vår rapport främst är fokuserad på användarna, och inte ingående behandlar de tekniska aspekterna av problemområdet, finner vi utrymme för fortsatt forskning med teknologin i fokus. Förslagsvis torde en vidare forskning om hur själva tekniken bakom NFC skyddar användaren mot säkerhetshot, t.ex. med hjälp av kryptering, vara angelägen. Dessa frågor av teknisk art hör snarare samman med andra forskningsområden än just informatik och faller därmed utanför ramarna för detta arbete.

Till vår undersökning finns det naturligtvis utrymme för ytterligare empiri, främst i form av intervjuer för att komplettera enkätundersökningen. Detta skulle kunna ge mer djup och en större förståelse för användarnas syn på säkerhetsaspekten. Dessutom skulle det vara intressant att inkludera hela åldersspannet i eventuella framtida undersökningar.

Bilaga A - Motivering av enkätfrågor

Nedan följer motivering av enkätfrågorna och ett kort resonemang om hur dessa är kopplade till teorin.

Fråga 1 – Kön

Frågan om kön finns med för möjligheten att urskilja skillnader i svaren, mellan könen. (kap 2.1.2)

Fråga 2 – Ålder

I avgränsningen (kap 1.4) för vi fram vår hypotes om de svarandes ålder i relation till enkäten.

Fråga 3 – Har du någonsin betalat med din mobiltelefon?

Fråga 4 – Om ”Ja”: Vilken metod använde du för att betala?

Fråga 5 – Om du svarade ”Nej” på föregående fråga: var vänlig motivera varför

I kap 2.1.1 nämner vi att SMS-betalning är den vanligaste betalningsmetoden i dagsläget och dessa frågor är menade att ta reda på om detta stämmer. Frågorna är även till för att se vilka anledningar som eventuellt hindrat de svarande från att betala med mobilen, enligt teorin i kap 2.1.3 torde säkerhet vara den främsta faktorn.

Fråga 6 – Är du intresserad av att betala med mobiltelefonen i framtiden?

Som vi förklarar i teorin (kap 2.1) förväntas mobilbetalningar användas för allt typ av försäljning i framtiden, syftet med frågan var således att ta reda på om det finns ett intresse hos användarna att bruka mobilen som betalningssätt i framtiden.

Fråga 7 – Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från ”Minst viktig” till ”Viktigast”.

Denna fråga är till för att jämföra de olika faktorerna för användaracceptans som beskrivs i kap 2.1.2. Vidare skall frågan även besvara huruvida säkerhet är den viktigaste av dessa, enligt användarna, som teorin beskriver i kap 2.1.3.

Fråga 8 – Hade du kunnat tänka dig att betala ”kontaktlöst” med din mobiltelefon?

Fråga 9 - Om du svarade "Nej" på föregående fråga, var vänlig motivera varför. Vill du lämna en kommentar till Ja-svaret går det också bra.

Frågan är en vidareutveckling av fråga 6, där vi vill se om användarna skiljer på mobilbetalning och kontaktlösbetalning. Som vi nämnde i kap 1.1 förutspås NFC bli den standard som kommer användas vid kontaktlös betalning och frågan är således även till för att se om användarna delar den uppfattningen.

Fråga 10 – Jag anser det troligt att en utomstående ”tjuvlyssnar” när jag genomför en kontaktlös betalning

Fråga 11 – Jag anser detta vara: ”inte särskilt allvarligt” till ”mycket allvarligt”

Fråga 12 - Jag anser det troligt att en utomstående stör kommunikationen när jag genomför en kontaktlös betalning

Fråga 13 – Jag anser detta vara: ”inte särskilt allvarligt” till ”mycket allvarligt”

Fråga 14 – Jag anser det troligt att min nuvarande position kan registreras utan min vetskap när jag genomför en kontaktlös betalning

Fråga 15 – Jag anser detta vara: ”inte särskilt allvarligt” till ”mycket allvarligt”

Fråga 16 – Jag anser det troligt att mina personliga uppgifter samt uppgifter om köp (t.ex. betalningshistorik) sparas och lagras vid kontaktlös betalning

Fråga 17 – Jag anser detta vara: ”inte särskilt allvarligt” till ”mycket allvarligt”

Fråga 10-17 är direkt kopplade till forskningsfrågan om hur medvetna användarna är om de säkerhetshot som finns inom NFC, samt hur de värderar dessa hot. Säkerhetshoten finns beskrivna i kap 2.4.3.

Fråga 18 – Vilket/vilka hot skulle hindra dig från att vilja betala kontaktlöst med din mobiltelefon?

Fråga 19 – Om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan jag INTE tänka mig att använda det

Dessa två frågor ämnar besvara vår underfråga om något av hoten kan vara ett hinder för spridningen av NFC som betalningsteknologi.

Bilaga B - Enkät

Mobilbetalningar med NFC

Hej! Vi är två studenter vid institutionen för Informatik på Lunds Universitet som skriver en kandidatuppsats om mobilbetalning. Kandidatuppsatsen kommer att behandla mobilbetalningar, NFC samt säkerheten hos teknologin. Vi försöker ta reda på hur användare ser på säkerheten och hur de värderar denna.

Därför ber vi dig svara på frågorna i vår enkät. Dina svar är en viktig del av vår undersökning! Vi vore väldigt tacksamma om du kan svara på vår enkät! Till sist vill vi framhålla att undersökningen är helt anonym! Inget du svarar kan kopplas till dig.

Många vänliga hälsningar Johan och Felix

Fråga 1. Kön *

- ○ *Man*
- ○ *Kvinna*

Fråga 2. Ålder *

- ○ 17 eller under
- ○ 18 - 25
- ○ 26 - 35
- ○ 36 - 45
- ○ 46 - 55
- ○ 56 - 65
- ○ 66 eller över

Fråga 3. Har du någonsin betalat med din mobiltelefon? *

- ○ Ja
- ○ Nej

Fråga 4. Om "Ja": Vilken metod använde du för att betala?

(Du kan kryssa i ett eller flera alternativ)

- ☐ Betalning med kontokort (Via webbläsaren)
- ☐ Betalning via mobilräkning (Premium SMS, betalsamtal m.fl.)
- ☐ Internetplånbok (eWallet t.ex. PayPal och Neteller m.fl.)
- ☐ Kontaktlös betalning (NFC)
- ☐ Övrigt:

Fråga 5. Om du svarade "Nej" på föregående fråga: var vänlig motivera varför

Fråga 6. Är du intresserad av att betala med mobiltelefonen i framtiden? *

- Ja
- Nej

Fråga 7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". *

Användarvänlighet: hur lätt mobilbetalningstjänsten är att använda. Pålitlighet och säkerhet: hur säker mobilbetalningen är. Användbarhet: vilken nytta mobilbetalningstjänsten har. Kostnad: hur mycket tjänsten kostar att använda. Kompabilitet: hur kompatibel tjänsten är med andra produkter och system.

	1 – Minst viktigt	2	3	4	5 - Viktigast
Användarvänlighet					
Pålitlighet och säkerhet					
Användbarhet					
Kostnad					
Kompabilitet					

Fråga 8. Hade du kunnat tänka dig att betala "kontaktlöst" med din mobiltelefon? *

(Kontaktlös betalning fungerar på samma sätt som när man använder ett JoJo-kort i kollektivtrafiken)

- Ja
- Nej

Fråga 9. Om du svarade "Nej" på föregående fråga, var vänlig motivera varför. Vill du lämna en kommentar till Ja-svaret går det också bra.

Tjuvlyssning

Tjuvlyssning innebär att en utomstående "lyssnar" på radiovågorna med exempelvis en antenn

Fråga 10. Jag anser det troligt att en utomstående "tjuvlyssnar" när jag genomför en kontaktlös betalning *

- Instämmer helt
- Instämmer delvis

- Varken eller
- Instämmer i någon mån
- Instämmer inte alls

Fråga 11. Jag anser detta vara *

	1	*2*	*3*	*4*	*5*	
Inte särskilt allvarligt						*Mycket allvarligt*

Störning

Störning innebär att en utomstående stör signalen för att till exempel göra det svårare att genomföra en betalning

Fråga 12. Jag anser det troligt att en utomstående ”stör” kommunikation när jag genomför en kontaktlös betalning *

- Instämmer helt
- Instämmer delvis
- Varken eller
- Instämmer i någon mån
- Instämmer inte alls

Fråga 13. Jag anser detta vara *

	1	*2*	*3*	*4*	*5*	
Inte särskilt allvarligt						*Mycket allvarligt*

Spårning

Spårning innebär att användarens mobiltelefons position registreras och att man på så sätt kan spåra användarens rörelser

Fråga 14. Jag anser det troligt att min nuvarande position kan registreras utan min vetskap när jag genomför en kontaktlös betalning

- Instämmer helt
- Instämmer delvis
- Varken eller
- Instämmer i någon mån
- Instämmer inte alls

Fråga 15. Jag anser detta vara *

	1	*2*	*3*	*4*	*5*	
Inte särskilt allvarligt						*Mycket allvarligt*

Lagring av information

Fråga 16. Jag anser det troligt att mina personliga uppgifter samt uppgifter om köp (t.ex. betalningshistorik) sparas och lagras vid kontaktlös betalning *

- Instämmer helt
- Instämmer delvis
- Varken eller
- Instämmer i någon mån
- Instämmer inte alls

Fråga 17. Jag anser detta vara *

	1	*2*	*3*	*4*	*5*	
Inte särskilt allvarligt	○	○	○	○	○	*Mycket allvarligt*

Fråga 18. Vilket/vilka hot skulle hindra dig från att vilja betala kontaktlöst med din mobiltelefon? *

(Du kan kryssa i ett eller flera alternativ)

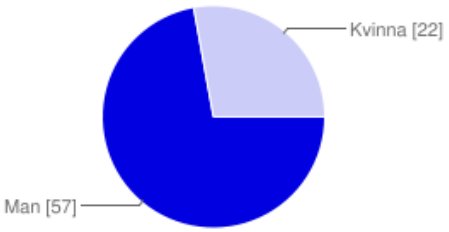
- ☐ Tjuvlyssning
- ☐ Störning
- ☐ Spårning
- ☐ Lagring av information
- ☐ Inget av ovanstående

Fråga 19. Om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan jag INTE tänka mig att använda det *

- Instämmer helt
- Instämmer delvis
- Varken eller
- Instämmer i någon mån
- Instämmer inte alls

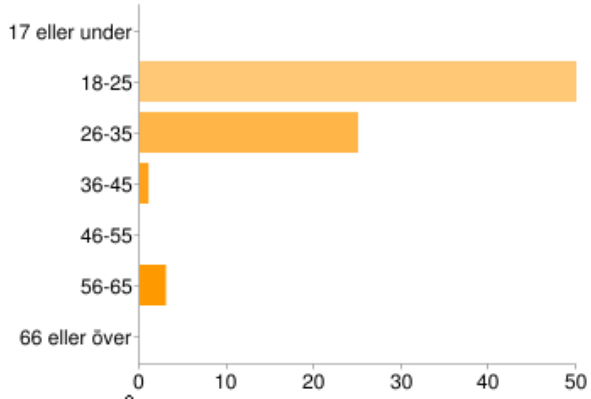
Bilaga C - Sammanställning av enkätsvar

1. Kön



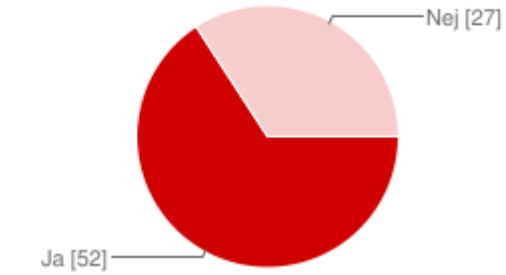
Man	**57**	72%
Kvinna	**22**	28%

2. Ålder



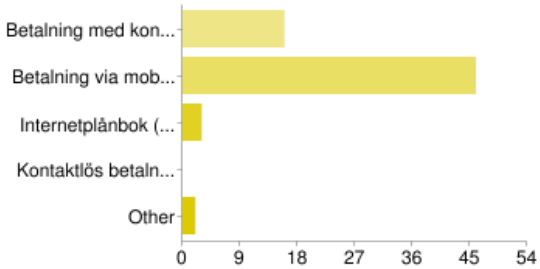
17 eller under	**0**	0%
18-25	**50**	63%
26-35	**25**	32%
36-45	**1**	1%
46-55	**0**	0%
56-65	**3**	4%
66 eller över	**0**	0%

3. Har du någonsin betalat med din mobiltelefon?



Ja	**52**	66%
Nej	**27**	34%

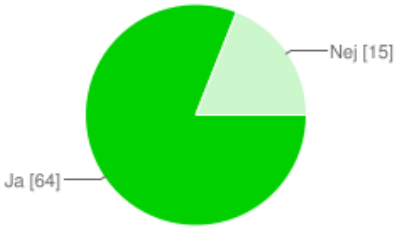
4. Om "Ja": Vilken metod använde du för att betala?



Betalning med kontokort (Via webbläsaren)	**16**	31%
Betalning via mobilräkning (Premium SMS, betalsamtal m.m.)	**46**	90%
Internetplånbok (eWallet t.ex. PayPal och Neteller m.fl.)	**3**	6%
Kontaktlös betalning (NFC)	**0**	0%
Other	**2**	4%

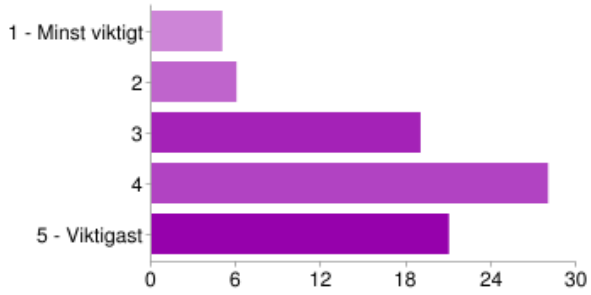
People may select more than one checkbox, so percentages may add up to more than 100%.

6. Är du intresserad av att betala med mobiltelefonen i framtiden?



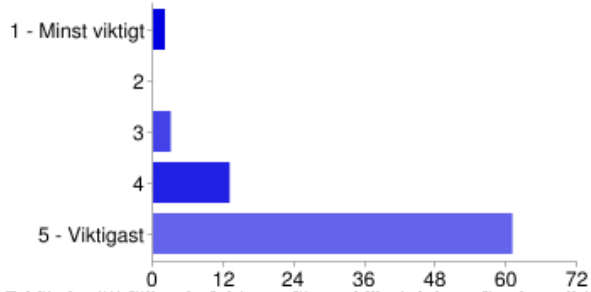
Ja	**64**	81%
Nej	**15**	19%

7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". - Användarvänlighet



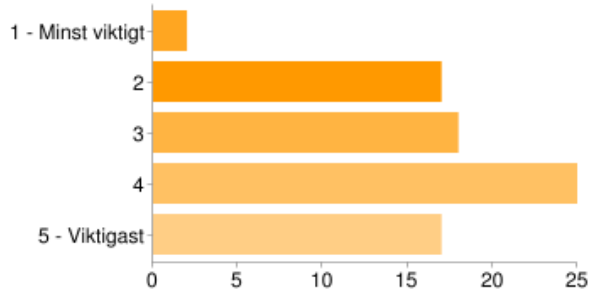
1 - Minst viktigt	**5**	6%
2	**6**	8%
3	**19**	24%
4	**28**	35%
5 - Viktigast	**21**	27%

7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". - Pålitlighet och säkerhet



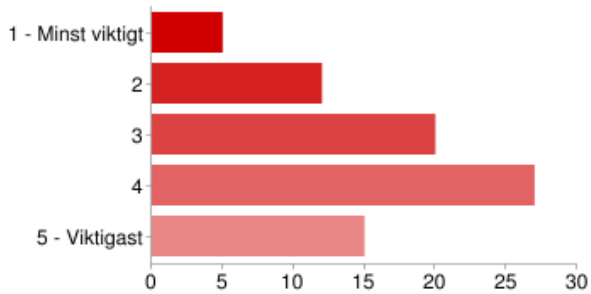
1 - Minst viktigt	**2**	3%
2	**0**	0%
3	**3**	4%
4	**13**	16%
5 - Viktigast	**61**	77%

7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". - Användbarhet



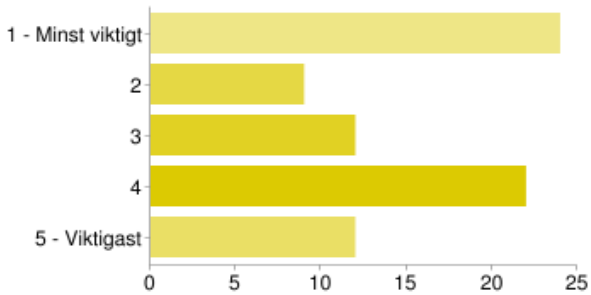
1 - Minst viktigt	**2**	3%
2	**17**	22%
3	**18**	23%
4	**25**	32%
5 - Viktigast	**17**	22%

7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". - Kostnad



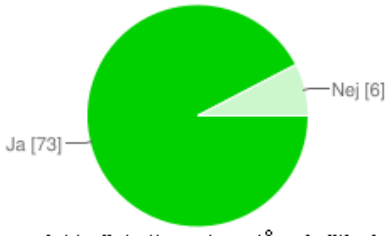
1 - Minst viktigt	**5**	6%
2	**12**	15%
3	**20**	25%
4	**27**	34%
5 - Viktigast	**15**	19%

7. Värdesätt följande faktorer för mobilbetalning efter hur viktiga du anser dem vara, från "Minst viktigt" till "Viktigast". - Kompabilitet



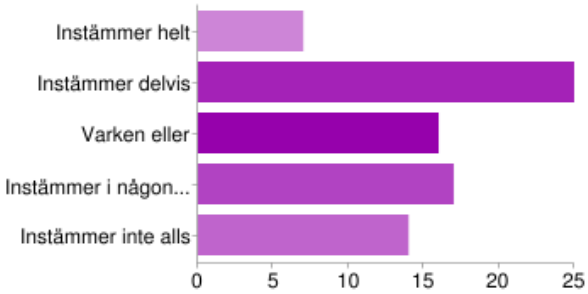
1 - Minst viktigt	**24**	30%
2	**9**	11%
3	**12**	15%
4	**22**	28%
5 - Viktigast	**12**	15%

8. Hade du kunnat tänka dig att betala "kontaktlöst" med din mobiltelefon?



Ja	**73**	92%
Nej	**6**	8%

10. Jag anser det troligt att en utomstående "tjuvlyssnar" när jag genomför en kontaktlös betalning

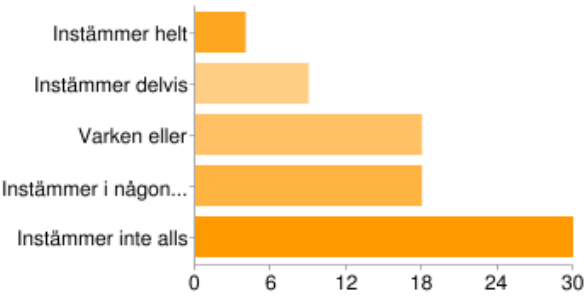


Instämmer helt	**7**	9%
Instämmer delvis	**25**	32%
Varken eller	**16**	20%
Instämmer i någon mån	**17**	22%
Instämmer inte alls	**14**	18%

11. Jag anser detta vara

1 -	Inte särskilt allvarligt	**4**	5%
2		**8**	10%
3		**10**	13%
4		**23**	29%
5 -	Mycket allvarligt	**34**	43%

12. Jag anser det troligt att en utomstående stör kommunikationen när jag genomför en kontaktlös betalning

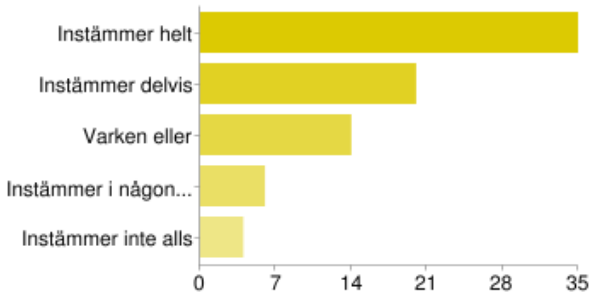


Instämmer helt	**4**	5%
Instämmer delvis	**9**	11%
Varken eller	**18**	23%
Instämmer i någon mån	**18**	23%
Instämmer inte alls	**30**	38%

13. Jag anser detta vara

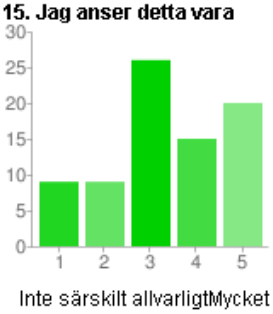
1 -	Inte särskilt allvarligt	**13**	16%
2		**18**	23%
3		**20**	25%
4		**17**	22%
5 -	Mycket allvarligt	**11**	14%

14. Jag anser det troligt att min nuvarande position kan registreras utan min vetskap när jag genomför en kontaktlös betalning



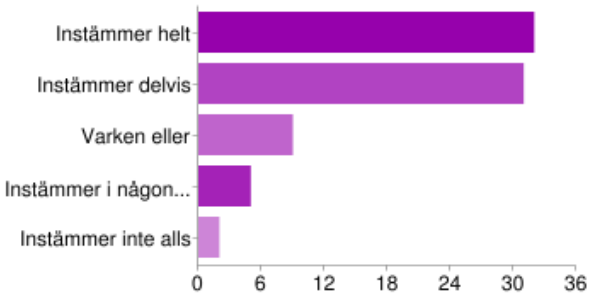
Instämmer helt	**35**	44%
Instämmer delvis	**20**	25%
Varken eller	**14**	18%
Instämmer i någon mån	**6**	8%
Instämmer inte alls	**4**	5%

15. Jag anser detta vara



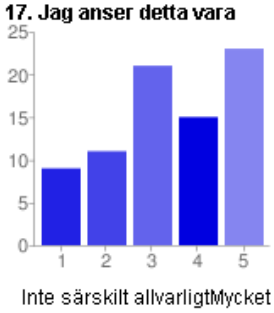
1 - Inte särskilt allvarligt	**9**	11%
2	**9**	11%
3	**26**	33%
4	**15**	19%
5 - Mycket allvarligt	**20**	25%

16. Jag anser det troligt att mina personliga uppgifter samt uppgifter om köp (t.ex. betalningshistorik) sparas och lagras vid kontaktlös betalning



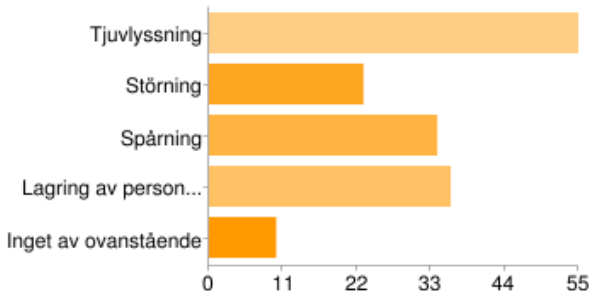
Instämmer helt	**32**	41%
Instämmer delvis	**31**	39%
Varken eller	**9**	11%
Instämmer i någon mån	**5**	6%
Instämmer inte alls	**2**	3%

17. Jag anser detta vara



1 - Inte särskilt allvarligt	**9**	11%
2	**11**	14%
3	**21**	27%
4	**15**	19%
5 - Mycket allvarligt	**23**	29%

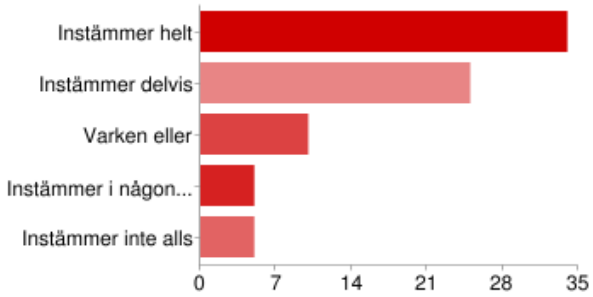
18. VilketMilka hot skulle hindra dig från att vilja betala kontaktlöst med din mobiltelefon?



Tjuvlyssning	55	70%
Störning	23	29%
Spårning	34	43%
Lagring av personlig information	36	46%
Inget av ovanstående	10	13%

People may select more than one checkbox, so percentages may add up to more than 100%.

19. Om kontaktlös mobilbetalning är mindre säkert än betalning med kreditkort så kan jag INTE tänka mig att använda det



Instämmer helt	34	43%
Instämmer delvis	25	32%
Varken eller	10	13%
Instämmer i någon mån	5	6%
Instämmer inte alls	5	6%

Fråga 5 - Om du svarade ”Nej” på föregående fråga: var vänlig motivera varför

”Min urgamla hajfenetelefon kan inte sådana fräcka trix!"

”Har försökt betala SJ-biljett med Visa genom webbläsare i iPhone, men inte kunnat slutföra.”

”verkar bättre och mer säkert att betala på annat sätt.”

”Inte haft behov”

”Betalar med mitt Visakort och för allt annat finns MasterCard men klart det kan va smart med även en lur, krävs dock ett pålitligt företag som kan ge oss denna tjänst bara.”

”Aldrig haft behov för det.”

”Jag har bara inte gjort det, har inte känt att det var behövligt.”

”Det låter läskigt att betala med mobilen men det låter ändå ganska fiffigt?”

”Har aldrig fått chansen...”

”Har aldrig kommit upp”

”Aldrig behövt eller haft möjlighet”

”Andra alternativ inövade, t.ex. internetbank.”

”Har helt enkelt inte funnits ngn anledning till att göra det.”

”ej insatt i teknologin ännu”

”Vet inte alls. Aldrig behövt det faktiskt. Hade inte haft några problem med att betala via kontokort eller paypal eller liknande.”

”har alltid haft en dator i närheten.”

”Gammal telefon.”

”Tillfället har inte dykt upp”

”Använder ingen smartphone för tillfället. Hade nog kunnat vara annorlunda annars med tanke på internettillgängligheten idag-.”

”för att det har aldrig varit aktuellt, betalar på annat sätt, alla mina räkningar betalas exempelvis via autogiro”

”Har inte haftbehovet!”

”ni menar förföregående fråga?”

”Jag går inte ut på nätet med min telefon. Jag betalar via datorn.”

Fråga 9 - Om du svarade "Nej" på föregående fråga, var vänlig motivera varför. Vill du lämna en kommentar till Ja-svaret går det också bra.

”jag är nöjd med mitt visa-kort”

”Känns osäkert”

”Jag svarade nej på frågan eftersom en sån funktion säkert kräver en modern, dyr och smart mobil. Många liknande funktioner förutsätter att man har en bra mobil, vilket är fruktansvärt irriterande. Inte alla vill lägga dyra pengar på sin mobil.”

”Ja: För att det har hänt att man har glömt plånboken hemma. Då skulle det vara perfekt att ha mobilen som räddning. ”

”Hade ju varit skitbra för småköp, typ bussen, en cola i läskautomaten och liknande.”

”känns osäkert. skulle nojja att den "piper" till då och då så att pengar dras.”

”Det beror främst på säkerheten vid köp.”

”vilken bra enkät!”

”Det känns inte riktigt säkert.”

”Ja med tvekan.Är tveksam om det kan vara säkert.”

”Hade varit smidigt. Ni borde kanske fundera på att lägga till en "kommentarer"- ruta i slutet med. :) Jag skriver här istället. Om tekniken börjar användas på allvar tror jag att problemet med tjuvlyssning osv kommer bli mycket större än det problemet vi har idag med skimming, om de inte kommer på något riktigt bra sätt att säkerhetställa genom kryptering eller whatever.”

”Låter farligt och jobbigt.”

”Det känns inte säkert.”

Referenser

Abdulhamid, F., & Hattab, E. (2008). A model for person-to-person electronic payment system.

Ackerman, M., Cranor, L. F., & Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *ACM Conference on Electronic Commerce - EC* (pp. 1-8). ACM Press.

Cleff, E. B. (2007). Privacy Issues in Mobile Advertising. *Internation Review of Law, Computers & Technology, 21*(3), 225-236.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Application, 7*(2), 165-181.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.* John Wiley & Sons.

Ejlertsson, G. (2005). *Enkäten i praktiken: en handbok i enkätmetodik* (2:a ed.). Lund: Studentlitteratur.

Frost & Sullivan. (2011). *Frost & Sullivan: Promised Marked for NFC Effectively Commences in 2011 with Commercial Roll out within All Verticals*. Retrieved 2011-05-12, from Frost & Sullivan: http://www.frost.com/prod/servlet/press-release.pag?docid=223107191

Gollman, D. (2011). *Computer Security.* Chichester: John Wiley & Sons.

Hanebeck, H.-C. L., & Raisinghani, M. S. (2003). Mobile Commerce: Transforming Vision into Reality. *Journal of Internet Commerce, 1*(3), 49-64.

Hard, H., Farahat, H., & Ezz, M. (2008). SecureSMSPay: Secure SMS Mobile Payment Model. *2008 2nd International Conference on Anti-counterfeiting, Security and Identification*, 11-17.

Haselsteiner, E., & Breitfuß, K. (2006). Security in Near Field Communication (NFC). *Workshop on RFID Security*.

He, Q., Wu, D., & Khosla, P. (2004). The quest for personal control over mobile location privacy. *IEEE Communications Magazine, 42*(5), 130-136.

Husemann, D. (1999). The smart card: don't leave home without it. *IEEE Concurrency, 7*(2), 24-27.

Innovision. (2007). *Near Field Communication in the real world – part II*. Retrieved 2011-05-12, from NFC Forum: http://www.nfc-forum.org/resources/white_papers/Innovision_whitePaper2.pdf

Jacobsen, D. (2002). *Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Lund: Studentlitteratur.

Li, S., Glass, R., & Records, H. (2008). The Influence of Gender on New Technology Adoption and Use-Mobile Commerce. *Journal of Internet Commerce, 7*(2), 270-289.

Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC Devices: Security and Privacy. *2008 Third International Conference on Availability, Reliability and Security*, 642-647.

Mallat, N. (2007). Exploring consumer adoption of mobile payments - A qualitative study. *The Journal of Strategic Information Systems*, 413-432.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of inititial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems, 11*(3-4), 297-323.

Microsoft. (2009). *Mobile Payments: Delivering Compelling Customer and Shareholder Value through a Complete, Coherent Approach*. Retrieved 2011-05-12, from Microsoft: http://www.microsoft.com/downloads/info.aspx?na=41&SrcFamilyId=9997243D-5F1B-405B-B0CB-F14ECDFB8566&SrcDisplayLang=en&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2f1%2f2%2fA%2f12AE1274-62EC-4BA0-86F1-7C36EB43FDF5%2fMobile_Payments_Whitepaper.pdf

Mulliner, C. (2009). Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. *International Conference on Availability, Reliability and Security*, 695-700.

Naumann, I., & Hogben, G. (2008). Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID).

NFC Forum. (2011). Retrieved 2011-05-12, from NFC Forum: www.nfc-forum.com

Nokia. (2007). Retrieved 2011-05-12, from Nokia: http://www.nokia.com/NOKIA_COM_1/Press/Materials/White_Papers/pdf_files/White%20paper_Nokia_Near%20field%20communication.pdf

Ok, K., Coskun, V., Aydin, M. N., & Ozdenizci, B. (2010). Current Benefits and Future Directions of NFC Services. *2010 International Conference on Education and Management Technology*, 334-338.

Ondrus, J., & Pigneur, Y. (2009). Near field communication: an assessment for future payment systems. *International Conference on the Management of Mobile Business, 7*(3), 347-361.

Pasquet, M., Reynaud, J., & Rosenberger, C. (2008). Payment with mobile NFC phones - How to analyze the security problems. *2008 International Symposium on Collaborative Technologies and Systems*.

Pedersen, A., Hedegaard, A., & Sharp, R. (2006). Designing a Secure Point-of-Sale System. *Fourth IEEE International Workshop on Information Assurance*, 15-65.

Pousttchi, K. (2008). A modeling approach and reference models for the analysis of mobile payment use cases. *Electronic Commerce Research and Applications, 7*(2), 182-201.

RFID Journal. (2011). Retrieved 2011-05-12, from RFID Journal: http://www.rfidjournal.com/

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Shivraj, K., & Vikas, J. (2008). Relationship between risk and intention to purchase in an online context: role of gender and product category.

Shon, T.-H., & Swatman, P. (1998). Identifying effectiveness criteria for Internet payment systems. *Internet Research: Electronic Networking Applications and Policy, 8*(3), 202-218.

Siau, K., Sheng, H., Nah, F., & Davis, S. (2004). A qualitative investigation on consumer trust in mobile commerce. *International Journal of Electronic Business, 2*(3), 283-300.

Stolpan. (2011). Retrieved 2011-05-12, from Stolpan: http://www.stolpan.com/

Su, Q. Y., & Li, X. W. (2010). Age/Gender/Occupation and Mobile Phone Technology Adoption: A Cross-Cultural Study in China (Beijing) And the UK (Portsmouth). *2010 International Conference on Management and Service Science*, 1-4.

Taghiloo, M., Ali Agheli, M., & Reza Rezaeinezhad, M. (2010). Mobile based secure digital wallet for peer to peer payment system. *International Journal of UbiComp, 1*(4), 1-11.

US-CERT. (2009). *United States Computer Emergency Readiness Team (US-CERT)*. Retrieved from Understanding Denial-of-Service Attacks: http://www.us-cert.gov/cas/tips/ST04-015.html

Valcourt, E., Robert, J.-M., & Beaulieu, F. (2005). Investigating mobile payment: supporting technologies, methods, and use. *Wireless And Mobile Computing, Networking And Communications, 4*, 29-36.

Yu, W. D., Nargundkar, S., & Tiruthani, N. (2008). A Phishing Vulnerability Analysis of Web Based Systems. *2008 IEEE Symposium on Computers and Communications*, 326-331.