Allmän uppfattning om kreditkortsäkerhet

Annika Melin Michael Niska
Email: {annme698,micni536}@student.liu.se
Supervisor: Viiveke Fåk, {viiveke@isy.liu.se}
Project Report for Information Security Course
Linköping University, Sweden
2010-05-05

Abstract

Credit cards are commonly used for payments where both the magnetic stripe and chip and pin can be used today. Six out of ten stores accept payments with chip whilst eight out of ten credit cards have chip in Sweden. This implies that the stores are limiting the higher safety that the chip and pin technique can provide. The reason for developing and implementing chip and pin was to minimize skimming. This is a fraud against the magnetic stripe on credit cards were the card's information is copied illegally.

The public perception in the survey is that chip and pin is safer than a magnetic strip. Also most of the people that answered the survey are aware of what skimming is. Though the risk acceptance varies the perception is that it is relatively safe to pay with a credit card in a store.

The responsibility is moved from the bank to the store when a credit card is exposed to fraud, in case a terminal that accepts chip and pin is not installed. This is an attempt made to encourage stores to install terminals accepting chip and pin but still there are stores in Sweden not using this technique. This means that credit cards with chip are not safer if used in stores only accepting payments with magnetic stripe or if the card gets stolen, as skimming still exists.

The people answering the survey are not that concerned about the fact that chip and pin is broken and thinks that it is relatively safe to pay with credit cards in stores. The reason for this perception could be that frauds against credit cards are not that common in Sweden. Another reason could be that they have good knowledge about the fact that it is the bank or the store that are responsible for paying when frauds occur and not themselves.

Sammanfattning

Kreditkort används i allt större utsträckning vid betalning där både magnetremsa och chip kan användas idag. Sex av tio butiker kan idag ta emot betalningar med chip medan åtta av tio kreditkort har chip i Sverige. Detta innebär att det i huvudsak är butikerna som förhindrar den förbättrade säkerheten som chipbetalning medför. Anledningen till att chip har utvecklats och införts är för att minska kreditkortsbedrägerier mot magnetremsa där kortets uppgifter som finns på magnetremsan kopieras olagligt, vilket kallas för skimming.

I allmänhet är de tillfrågade i enkätundersökningen medvetna om att chip är säkrare än magnetremsa och vad skimming innebär. Däremot varierar riskacceptansen medan uppfattningen är att det är relativt säkert att betala med kreditkort i butik.

Ersättningsansvaret vid kreditkortsbedrägeri har överförts från banken till butikerna om inte butikerna installerat betalterminaler med chip. Detta i syfte att uppmuntra butikerna att installera chipterminaler men fortfarande finns det butiker som inte använder denna teknik. Detta innebär att kort med chip inte är säkrare vid betalning i butik som endast tar emot betalning med magnetremsa eller om kortet blir stulet.

Att de tillfrågade i allmänhet inte är speciellt oroade över att chipfunktionen är knäckt och tycker att det är relativt säkert att betala med kort i butik kan bero på att det i Sverige inte är speciellt vanligt med kreditkortsbedrägeri. En annan orsak kan vara att de är medvetna om att de själva inte står för kostnaden utan att banken eller butiken gör detta.

1. Introduktion

I detta inledande avsnitt presenteras bakgrund och syfte med rapporten. Vidare presenteras vilken metod som använts samt på vilket sätt rapporten sammanställts. Avslutningsvis gås metod- och källkritik igenom.

1.1 Bakgrund

Säkerheten vid kortbetalning blir alltmer ifrågasatt ju fler kortbedrägerier som uppdagas i media. Så kallad skimming av kreditkort innebär att informationen på kreditkortets magnetremsa kopieras och kan exempelvis ske på restaurang, i butik eller i en uttagsautomat. Bedragaren kan därefter utnyttja det kopierade kreditkortets information och använda det för att olovligt köpa varor eller göra uttag. Det finns idag mycket

sofistikerade lösningar[1] på att skimma kort, och det existerar brottsliga organisationer som lever på kreditkortsbedrägerier.

För att åtgärda problemet med kreditkortsskimming framtogs en ny och säkrare metod för kortbetalning; kreditkortsbetalning med chip. Detta infördes för ett antal år sedan för att öka säkerheten för kortbetalning men har hittills inte utnyttjats i sin fulla potential. Under år 2009 kunde endast 20 % (1) av Sveriges butiker med betalterminal ta emot chip medan denna siffra idag är 60 % (2). Forskare har länge menat att chipanvändningen är mycket säkrare jämfört med användning av magnetremsan vid betalning med kort. Nyligen har dock fortskare vid Cambridges universitet kommit fram till att ett protokoll i chipterminalens mjukvara kan vara knäckt (3).

1.2 Syfte

Syftet med rapporten är att undersöka användares uppfattning om säkerhet och risknivå hos kreditkort och kortbetalningar samt väga det mot teorin och forskares uppfattningar.

1.3 Metod

I detta avsnitt presenteras den metod som ska användas för att sammanställa rapporten. Metoden indelas i en teoretisk del och en praktisk del. Den teoretiska bygger på informationsinsamling av kvalitativ art medan den praktiska består av informationsinsamling av kvantitativ art samt hur informationsinsamlingen skall gå tillväga.

1.3.1 Teoretisk

Kvalitativ data hämtas från facklitteratur, artiklar och Internetsidor som behandlar säkerhet och risknivåer vid kortbetalning. Utöver detta beskrivs även vikten av autentisering och teorierna bakom detta. I biblioteks-databaser har en artikel- och facklitteratursflora insamlats vars innehåll senare sammanställs till en referensram. Referensramen ligger senare till grund för den analys som skall utföras där resultatet av en enkätundersökning analyseras och vägs mot teorin.

1.3.2 Praktisk

För att väga in kvantitativ data har en enkät om kreditkortsanvändning framtagits och finns bifogad i slutet av rapporten som bilaga 2. Enkäten ämnar svara på ett antal frågeställningar som författarna själva ställt sig. Några av dessa frågeställningar är:

- I hur stor utsträckning är chipfunktionen fungerande?
- Hur ofta sker betalning med chip respektive magnetremsa?
- Huruvida användarna av bankkort känner till tekniken bakom magnetremsa och chip på betalkort samt dess säkerhetsskillnader.

Utöver detta får användarna gradera sin egen uppfattning av riskerna med betalkort, vilken risknivå som accepteras, hur säkert användarna anser att kortbetalning är samt hur viktig säkerheten med betalkort anses vara.

Enkäten riktar sig mot två målgrupper. De som handlar med betalkort, senare i rapporten kallade användare, samt de som arbetar i butik. Dessa målgrupper kan vara samma person. Dock är denna indelning av vikt då undersökningen kan visa på olika förståelse för riskerna och säkerheten vid kreditkortsbetalning. Undersökningen har utförts utanför olika butiker i Linköpings omnejd där användare tillfrågas att besvara enkäten efter utförd inhandling. Butikernas personal har även de tillfrågats för att en jämförelse ska kunna göras.

Vidare har utvalda personer kontaktats i andra svenska städer för att öka den geografiska spridningen. Ett försök gjordes att kontakta de butiker där användare som ifyllt enkät handlat, där en butiks personal ställde upp. Detta gjordes i syfte att få tillgång till butikens anställdas åsikter och kunna jämföra dessa.

Vid sammanställning av resultatet har jämförelser av kunskap, förståelse och intresse för betalkorts funktionalitet, säkerhet och risknivå genomförts fördelat på kön, ålder och roll i undersökningen. Utifrån resultatet sammanvägdes svaren mot teorin för att ge svar på användares kunskap om säkerhet och risknivå vid kortbetalning, vilket gav svar på i vilken grad kortbetalning utnyttjas och uppskattas för användare i olika åldrar och av olika kön.

Ett första utkast togs fram varefter det testades på fem personer för att ta reda på om enkäten var enkel att förstå och tydlig. Med hänsyn till de kommentarer som erhölls, arbetades den slutgiltiga versionen fram, där förtydligande text lagts till samt omformuleringar gjorts för att eliminera tvetydiga frågor och missförstånd.

1.3.3 Metodkritik

Genomförd enkätundersökning har högre svarsfrekvens från målgruppen kunder än från målgruppen som jobbar i butik. Därmed är resultatet som presenteras för kundgruppen mer rättvisande än den för butiksarbetande och de jämförelser som görs målgrupperna emellan inte

[1] Den intresserade läsaren kan läsa följande artikel angående en sofistikerad lösning för att kopiera kreditkortsinformation:
http://www.krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/

helt rättvisa, men ger en fingervisning på skillnaderna om säkerhetsmedvetenheten rollerna emellan.

Vissa av kunskapsfrågorna i enkäten har besvarats jakande medan fel fakta därefter angivits. Exempelvis besvarades frågan ”Vet du vad skillnaden i teknik är mellan magnetremsa och chip är?” ibland jakande medan beskrivningen av teknikskillnaden inte var relevant eller felaktig. Detta visar på att resultatet kan vara något missvisande då personer fyllt i att de besitter en kunskap som de i själva verket inte gör.

Informations- och faktasökning på Internet är krävande då det inte finns mycket sammanställt inom ämnet. Därmed har referenssamling varit krävande och tagit mycket tid då många olika Internetsidor utforskats. Andra alternativ för faktainsamling, om dessa hade varit kända innan rapportens start, hade eventuellt varit mer effektiva.

1.4 Källkritik

Endast en av källorna som använts i detta projekt är facklitteratur inom ämnet. Resterande material har insamlats på olika Internetsidor som saknar akademisk tyngd men däremot är unga samt relevanta för ämnet och därmed är högaktuella.

1.5 Avgränsning

Kreditkort används vid olika tillfällen såsom betalning för varor i butik, uttag av kontanter från konto i bankomat samt vid betalning via Internet. Då möjligheten att betala med magnetremsa eller chip endast gäller vid fysisk betalning i butik avgränsar vi oss dit med tanke på syftet – att undersöka allmänhetens uppfattning om kortsäkerhet i ett perspektiv av magnetremsa i jämförelse med chip.

Vi har även begränsat oss till att undersöka hur situationen i Sverige ser ut. Att väga in andra länder är alltför tidskrävande i förhållande till kursens storlek. I första hand fokuseras Linköping som stad men avvikelser från detta kan förekomma då personer som deltar i undersökningen nyligen kan ha besökt annan stad. Linköping kan anses vara representativ som stad då den med sin storlek och befolkning inte skiljer sig nämnvärt från andra svenska städer.

2. Historik

Från början utvecklades kreditkortet som en ersättning till kontanter eller check samt för att underlätta uttag av kontanter från bankkonton. Sedan några år har även betalningar via internet möjliggjorts tack vare kreditkortet (4).

Magnetremsans teknik började användas i början 1960-talet då ett magnetremsesystem installerades i Londons tunnelbana. Kreditkorten användes redan i början av 1950-talet, men det var inte förrän 1970 som magnetremsan blev ett inslag på kreditkortet (5).

Det finns i Sverige idag mer än 16 miljoner kreditkort av vilka alla har magnetremsa. Denna har varit standard i flera decennier nu och var även det enda betalalternativet under denna period (6). Det har dock visat sig att magnetremsan är lätt att kopiera, då kortet kan utsättas för så kallad skimming. Bedragare kopierar i dessa fall information från magnetremsan och använder denna information för att komma åt pengar eller köpa varor (7). För att kopiera ett kort med magnetremsa krävs en kreditkortsterminal, som endast kostar några tusenlappar (8).

För att svara mot denna säkerhetsrisk utvecklades en ny betalningsmetod för kort: kreditkortsbetalning med chip. Magnetremsan försvann inte i och med detta utan kreditkortet kompletterades med ett chip. Idag har cirka 80 % av alla kreditkort chip och meningen är att alla kreditkort ska vara utrustade med chip i framtiden. Anledningen till detta är att chip är säkrare än magnetremsan samt att mer information ryms på chipet jämfört med magnetremsan (7). Chipet är säkrare i det avseende att det är svårare att förfalska än magnetremsan och drabbas därmed inte lika ofta av bedrägerier (6). I Sverige började de första bankerna förse betalkort med chip i början av 2000-talet, vilket är mycket senare än resten av Europa. En anledning till detta är att skimming inte har varit lika vanligt i Sverige som övriga Europa. (9)

Kreditkort har i dagsläget både magnetremsa och chip då alla kortläsare i butik fortfarande inte kan läsa chip, som inom en snar framtid ska bli ny standard (10). Eftersom magnetremsan fortfarande måste vara och finns kvar på alla kreditkort, kan de fortfarande utsättas för skimming, om inte butiken använder sig av chipbetalning. Enbart ett chip på kreditkortet innebär en väldigt liten risk för bedrägerier, medan kombinationen av magnetremsa och chip försämrar säkerheten. Korten med båda är dock säkrare om de endast används i betalterminaler som bara läser chip (8). När alla dessa betalterminaler kan läsa chip, kommer bankerna istället kunna tillverka kreditkort som endast har ett chip och ingen magnetremsa, vilket innebär att kreditkort inte längre kan utsättas för skimming och därmed är säkrare att använda (7).

Endast ca 60 % av betalkortsterminalerna har chipläsare idag. Större butikers betalsystem har svårigheter att integrera betalning med chip vilket gör att betalning med magnetremsa hänger kvar trots säkerhetsriskerna. En annan anledning till att chipbetalning inte används till 100 % trots säkerhetsaspekterna kan vara att de svenska kunderna ej sätter press på butikerna i dagsläget, vad gäller betalning med chip istället för magnetremsa. Detta i sin tur kan bero på att svenska användare inte utsätts för kortbedrägerier i lika hög grad jämfört med övriga Europa, enligt undersökningar, och därmed inte upplever någon större skillnad mellan användning av magnetremsa

och chip (11). Den 1:a januari 2009 blev alla butiker och handlare ersättningsskyldiga om ett bedrägeri skulle ske i deras butik. Detta om de inte hade bytt ut sina betalterminaler mot sådana som godtar både magnetremsa och chip. I och med att alla butiker fortfarande inte gjort detta måste betalkorten som utfärdas idag både ha magnetremsa och chip. Butikerna måste därmed ta sitt ansvar för att användarna ska kunna göra betalningar i butik med chip istället för magnetremsa (6).

3. Referensram – Magnetremsa vs chip

I referensramen behandlas litteratur i ämnet om magnetremsa och chip i avseendena tekniska skillnader, risker och konsekvenser.

3.1 Tekniska skillnader

Här följer en kortfattad teknisk beskrivning av magnetremsa och chip för att ge läsaren en förståelse för de grundläggande skillnaderna.

3.1.1 Magnetremsa

Tekniken i magnetremsan är känd som ett enkelt och kostnadseffektivt sätt att lagra en mängd omskrivbar och maskinläsbar data med hjälp av magnetisk lagringsteknik (5). Magnetremsan är en mycket tunn filmremsa som har förmågan att lagra digital information, det vill säga ettor och nollor. Materialet är detsamma som materialet i VHS-kasetter. När magnetremsan används dras den genom en terminal där ettorna och nollorna översätts till en nummerföljd. Denna nummerföljd är helt unik för innehavaren, vilken kan spåras till ett knutet bankkonto där pengarna ska dras ifrån (6).

3.1.2 Chip

Chiptekniken kallas för EMV då Europay, MasterCard och VISA ligger bakom den. Ett chip fungerar som en dator och kan lagra stora mängder information, mer än en magnetremsa kan lagra. Vid betalning när kreditkortet sticks in i terminalen kommunicerar terminalen direkt med kortets chip och det data som finns lagrat där (12).

Vid transaktionstillfället med chip kontrolleras att kortet är den genuina artikel det påstår sig vara och att den person som använder kortet är den riktiga ägaren. Chipet gör det effektivt omöjligt att förfalska eller kopiera kortet medan pinkoden gör det svårare för kriminella att använda ett borttappat eller stulet kort (13).

3.2 Skimming

Den vanligaste och mest kända risken ett kreditkort kan utsättas för är så kallad skimming. Anledningen till att magnetremsa håller på att bytas ut mot chip är på grund av säkerhetsriskerna med magnetremsa på kreditkort. Den vanligaste metoden för kortbedrägerier är skimming (6).

Skimming innebär att bedragare genom falska betalterminaler, som endast kostar några tusenlappar och är lätta att få tag på, kopierar information som finns på kreditkortets magnetremsa. Informationen kopieras när användaren för in sitt kort i vad den tror är en vanlig betalterminal, men det egentligen är en falsk betalterminal. Bedragaren kan därefter använda informationen från magnetremsan för att köpa varor eller ta ut pengar.

En terminal som mottar chip vid betalningstillfället är mer eller mindre omöjlig att förfalska, vilket gör att kreditkort med chip är att föredra (6).

3.3 EMV – protokollet som knäcktes

Det idag ledande systemet för kreditkort är EMV, som står för Europay, Mastercard och Visa. Systemet utnyttjas i princip i hela Europa och 730 miljoner EMV-kort finns i dagsläget världen över. Kortet består, förutom en magnetremsa, av ett chip som verifierar transaktioner med hjälp av en pinkod. Pinkoden, som knappas in i terminalen vid betalningstillfället, verifieras av EMV-kreditkortet, som i sin tur verifieras av ett digitalt certifikat i betalningsterminalen. Detaljinformation om transaktionen som sänds verifieras med MAC (message authentication code), med hjälp av en symmetrisk nyckel, och måste vara korrekt för att betalningen ska kunna genomföras. Den symmetriska nyckeln kan inte läsas ut ur kortet utan delas endast mellan kreditkortet och banken som utgivit kreditkortet (3).

EMV-kreditkortet togs fram med avsikten att minska kreditkortsbedrägeri där chippet skulle motstå kort-förfalskning och pinkoden skulle motstå användningen av stulna kort. Detta har fått effekten att antalet stulna kreditkort har minskat och kreditkortförfalskning haft en tvåårig paus. Dock har bedrägeriet inte eliminerats utan generellt ökat enligt brittisk statistik och tecken visar fortfarande på en ökning (3).

Målet med EMV var att minska bankers kostnader för tvister och ersättning som uppkommer vid kortbedrägerier på ett sätt så att affärsinnehavaren skulle stå för kostnaden vid förfalskad signatur och kunden skulle stå för kostnaden om den falska transaktionen genomfördes med pinkod. Detta har gett effekten att bankerna, som är de ansvariga för designen av systemet, nu inte har samma skyldighet och ansvar vid kortbedrägeri. Säkerhetschefer (security economics) anser att detta kan skapa moraliska dilemman genom att bankerna isoleras från ansvar för ett dåligt designat system (3).

Flertalet tidningar och artiklar har behandlat och diskuterat tekniska attacker mot EMV-kreditkort. Idag är systemet dock så djupt etablerat på marknaden att systemändringar kan bli svåra att göra. Ändringar i säkerhetsprotokoll och mjukvara involverar allt från

banker och affärsinnehavare till kort- och kortläsar-tillverkare, som alla jobbar hårt för att skydda sina egna intressen. Systemet är idag fyllt av suboptimala designbeslut skapade ett decennium tillbaka och detta är vi fast vid (3).

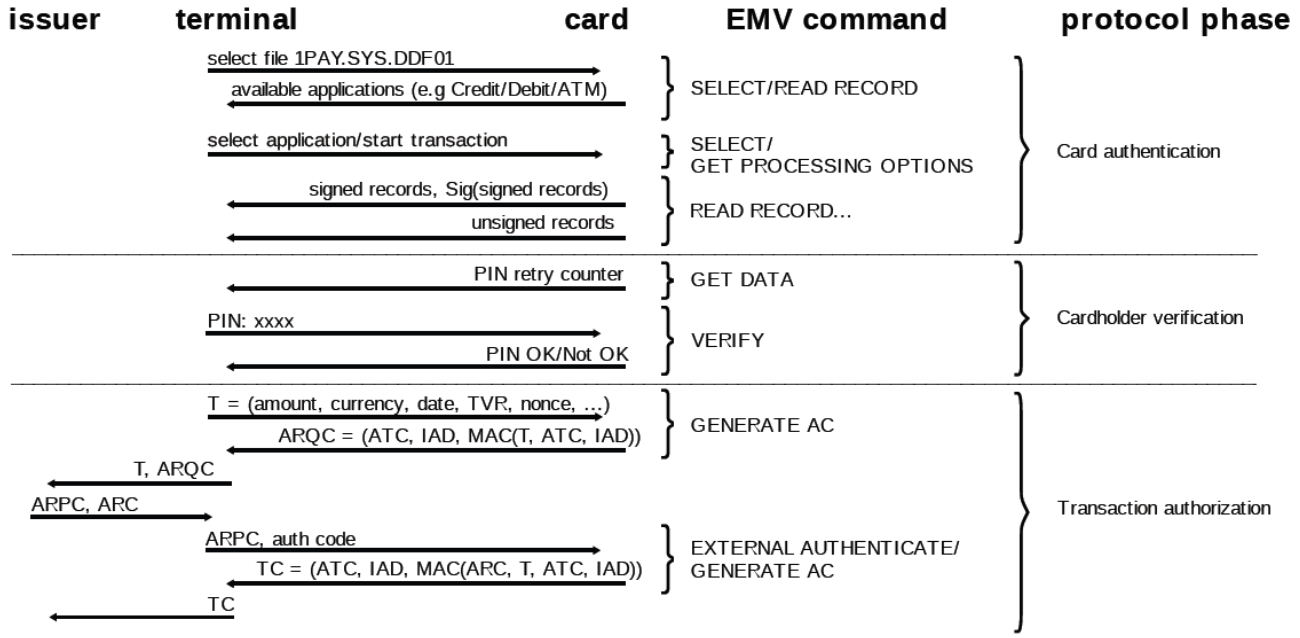
3.3.1 Protokollet knäckt

EMV är både ett antal protokolldefinitioner (protocol suite) och en generell verktygslåda utifrån vilket man kan bygga protokoll (proprietary protocol framework). Praktiskt fungerar det som följer: Banken som tillhandahåller EMV-kreditkortet väljer en delmängd av EMV-protokollen, väljer exempelvis mellan digitala signaturmetoder, MAC algoritmer samt väljer mellan hundratals skräddarsydda alternativ gällande verifiering och risk management. Samtidigt står affärsinnehavare och banker för den hårdvara som ska kommunicera med den sammansatta EMV-strukturen. Det som hänt är att ett protokoll knäckts för både brister i EMV-verktygslådan och för brister i ägarprotokollen tillhörande MAC, som i sin tur utfärdas av bankerna. EMV protokollet kan delas in i tre faser, vilket visas i Figur 1 nedan.

Card Authentication: Försäkrar betalterminalen vilken bank som utfärdat kreditkortet och att data på kortet inte manipulerats med.

Cardholder verification: Försäkrar betalterminalen att den pinkod som angetts av kunden matchar den kod som lagrats på kreditkortet.

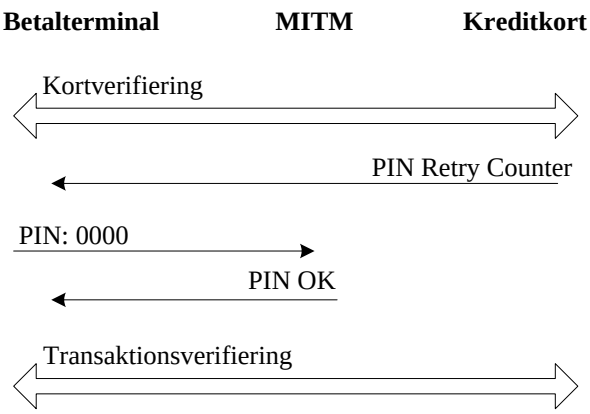
Transaction authorization: Försäkrar betalterminalen att banken som utfärdat kreditkortet tillåter transaktionen att gå igenom (3).



Figur 1. Komplett körning av chipets protokoll vid kreditkortstransaktion

3.3.2 Kreditkortsattacken (the attack)

Den centrala bristen i protokollet är att tillvägagångssättet vid pinkodsbekräftelsen inte tydligt verifieras. Verifierad data som sänds till banken består av två fält som innehåller information om resultatet av kreditkortinnehavarens bekräftelse (Terminal verification result, TVR, och issuer application data, IAD). Tillsammans utgör dock dessa inte en otvetydig avkodning av vad som hänt. Därför kan en ”man-in-the-middle”-apparat (MITM) lura betalterminalen att tro att pinkoden bekräftats utan att pinkoden sänts till kreditkortet. En dummy pinkod måste matas in, men attacken tillåter vilken pinkod som helst att passera och transaktionen går igenom. Kreditkortet tror då att betalterminalen inte stödjer pinkodsverifiering och då struntat i att verifiera kortinnehavaren eller utnyttjat signatur istället. Eftersom dummy pinkoden aldrig sänds till kreditkortet så aktiveras aldrig ”PIN retry counter”, som visas i Figur 2. (3)



Figur 2. man-in-the-middle undertrycker pinkodsverifieringen hos kreditkortet och meddelar betalterminalen att pinkoden verifierats korrekt. (3)

Varken kreditkortet eller betalterminalen känner av detta eftersom kreditkortsinnehavarens verifieringsbit (byte) i TVR endast aktiveras om pinkodsverifieringen misslyckats. Betalterminalen tror att pinkodsverifieringen lyckats och kreditkortet tror att densamma aldrig provats och accepterar därför den information som betalterminalen sänder till kreditkortet. På så sätt får varken kreditkortet, betalterminalen eller kreditkortsutgivaren tillräcklig information till att upptäcka kortbedrägeriet (3).

3.3.3 Orsaker

Den identifierade bristen med chip och pin kan skyllas på mycket, men i grunden beror den på ett fundamentalt protokollmisslyckande inom EMV-tekniken. Detta misslyckande grundar sig i att det utfärdar-specifika MAC protokollet avdelas för distinkt från kortägarens verifikationsmetod. Både butiken och banken, som förlitar sig på transaktionsverifieringen, behöver pålitlig och full insyn av resultatet av kortägarens verifikationsmetod. Då denna data ej kan sammanställas på ett enkelt sätt av någon av parterna, brister strukturen i protokollet med hänsyn till säkerheten. Nyckelmissuppfattningen som designerna gjorde var att tänka på TVR (terminal verification result) och resultatet av kortverifikationen som separata listor med möjliga misslyckanden, istället för att tänka på dem som en följd i rapportering av verifieringsprotokollet (3).

3.4 Varför chip är säkrare än magnetremsa

Beskrivet tidigare i texten är att både magnetremsa och chip kan utsättas för bedrägeri. Vid betalningstillfälle i butik läses kortets magnetremsa av i betalterminalen, att kopiera information från en magnetremsa kan göras relativt lätt med billig utrustning som är lätt att få tag på. Bakom bedrägeriet kan antingen en butiksanställd eller en utomstående person stå. Om kortet blir stulet kan informationen på magnetremsan kopieras till ett nytt kort eller användas i butik med falsk signatur (3).

Vid kortbetalning i butik med chip verifieras både pinkoden och kortet. Den pinkod som knappas in i betalterminalen verifieras av kontokortet och kortet verifieras av betalterminalen. Därefter verifieras transaktionen av banken genom en symmetrisk nyckel som delas med kortet. Information kan inte läsas av eller kopieras från chip och därmed kan inte kortinnehavaren, under tiden denne betalar med chip, utsättas för bedrägeri. Däremot kan kort med chip utsättas för den attack som tidigare beskrivits, där den riktiga pinkodsverifieringen slås ut. För att kunna genomföra en sådan attack behövs både ett stulet, eller upphittat, kort och teknisk utrustning. Denna utrustning är idag ovanlig i jämförelse mot skimmingutrustningen och mer tekniskt komplicerad då den både bedrar betalterminalen och kortet (3).

Det är i de flesta butiker obligatoriskt att använda pinkod tillsammans med chip men det finns butiker där det är möjligt för kortinnehavaren att välja signering som verifiering istället. Därmed kan även chipbetalningar i sällsynta fall göras av någon annan än kortinnehavaren, en bedragare som stulit eller hittat ett kort, utan teknisk utrustning och med falsk signatur (3).

Vid betalningstillfället är det således i nuläget en stor skillnad i säkerhet mellan betalning med magnetremsa och betalning med chip. Magnetremsan riskerar att kopieras medan chipet är säkert mot detta. Det är först när kortet är borttappat eller stulet som chipet löper risk för bedrägeri (3).

Ett borttappat eller bestulet kort kan därmed utsättas för bedrägeri både gällande magnetremsa och chip. Magnetremsan kan kopieras av eller användas i butik med falsk signatur. Chipet kan användas med pinkod om bedragaren fått reda på denna, med falsk signatur om butiken tillåter signering som verifiering samt utsättas för attacken där bedragaren använder teknisk utrustning för att förbigå den äkta pinkodsverifieringen. Detta påvisar att chipet löper mycket mindre risk att utsättas för bedrägeri än magnetremsan vid fall av borttappat eller bestulet kort (3).

Korten har idag fortfarande både magnetremsa och chip vilket innebär att ett kort med chip fortfarande löper samma risker som ett kort med endast magnetremsa om kortet tappas bort eller blir stulet samt om det används i butik som endast använder sig av betalning med magnetremsa. Det är endast vid betaltillfället i butik, som accepterar chipbetalning, som det är mycket säkrare att ha ett kort med chip (3).

3.5 Konsekvenser

Nedan följer en beskrivning av vilka konsekvenser användaren står inför vid olika slags realiserade risker som har att göra med kreditkortet.

3.5.1 Förlust av kort

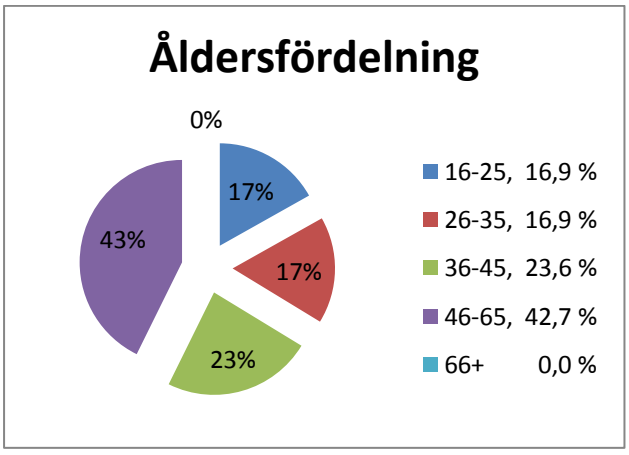
Efter att kortanvändaren utsatts för kortförlust bör detta rapporteras så snabbt som möjligt. Detta då belopp som berör kontot efter det att förlustanmälan mottagits ej belastar användaren. Innan en anmälan kommit in kan kortanvändaren bli betalningsansvarig för de belopp som rör kontot om denne lämnat ifrån sig kortet till någon annan, genom grov oaktsamhet förlorat kortet eller inte snarast, efter förlustupptäckten, anmält kreditkortet försvunnet. Efter en förlustanmälan spelar alltså ej dessa någon roll, utan endast om användaren har gjort sig skyldig till svek blir denne betalningsansvarig (4).

3.5.2 Ersättningsansvar

Den första januari i år blev alla butiker och handlare ersättningsskyldiga om ett bedrägeri skulle begås i deras butik. Detta om de inte hade bytt ut sina betalterminaler mot sådana som godtar både magnetremsa och chip. Genom att förflytta ersättningsansvar till butikerna ska de motiveras att införskaffa betalterminaler som även tar emot chip, vilket i sin tur är säkrare för kunderna som kan betala med chip istället för den mindre säkra magnetremsan (6). Dessförinnan hade bankerna som inlösare det ekonomiska ansvaret för kreditkorts-bedrägerier som hade kunnat förhindras med en chipterminal i butikerna (14).

4. Resultat

Enkätresultatet som presenteras i detta avsnitt grundar sig på 89 enkätsvar som besvarats av 56 % män och 44 % kvinnor. Dessa personer har en åldersfördelning enligt Figur 3 nedan.



Figur 3. Åldersfördelning bland enkätsvar

Utav dessa personer är 73 stycken kunder i olika butiker samtidigt som 16 stycken arbetar i butik. Bland samtliga deltagare föredrog 84 % att betala med kreditkort jämfört med att använda kontanter, där endast personer äldre än 36 år föredrog kontanter. Samtliga deltagare har idag ett kreditkort med både chip och magnetremsa och 99 % av deltagarna ansåg att kreditkortsbetalning fungerar på ett tillfredsställande sätt. Av de tillfrågade betalar 89 % alltid eller oftast med kreditkort. Samtidigt ansåg 63 % att betalning med chip endast förekom ibland eller mer sällan än så, vilket framgår av Tabell 1 nedan.

Tabell 1. Kreditkortsbetalning, varav med chip

	Kreditkortsbetalning	Med chip
Aldrig	0%	0%
Sällan	4%	12%
Ibland	7%	51%
Oftast	72%	37%
Alltid	17%	0%

Frågor ställdes angående de medverkandes senaste betalning i butik, varvid det i 86 % av fallen betalades med kreditkort. Av dessa 77 fall betaldes det i 63 % av fallen med magnetremsa då chipfunktionen antingen var trasig (1 fall) eller ännu inte i bruk (44 fall).

Få känner till de tekniska skillnaderna mellan chip och magnetremsa. I vår undersökning ansåg 11 % av deltagarna sig veta de tekniska skillnaderna, men då personerna försökt beskriva skillnaderna har det visat att deras tro inte stämmer och i själva verket vet än färre de tekniska skillnaderna. Angående säkerhetsskillnaderna chip och magnetremsa emellan visste 30 % av deltagarna de tekniska skillnaderna, dock endast på en ytlig nivå som att chip är säkrare. Fler än hälften av deltagarna (69 %) hade någon gång hört talas om vad skimming är och deras förklaring av bedrägeriet var väl överensstämmande med dess korrekta definition. Dock kände endast en fjärdedel av de tillfrågade till att ett protokoll i chippet knäckts.

Användares allmänna uppfattning om kreditkortssäkerhet med magnetremsa varierar över den femgradiga skalan, med största vikt mellan 2-4. Kort med chip uppfattas dock säkrare där 70 % av användarna uppfattar säkerheten på nivå 4 eller högre på en femgradig skala. Säkerheten i butik uppfattas dock som högre än den allmänna då användaren då säger sig ha koll på kortet under hela transaktionen, vilket gör att betalningsförloppet känns tryggare. I princip samtliga användare som deltagit i enkäten trycker på vikten av att kreditkortet är säkert att använda, men användarna uttrycker en oro vid kortanvändning då de besvarat frågor kring deras

uppfattning av riskerna gällande kreditkortsbetalning. Risker i butik rankas lägre än riskerna i allmänhet. Dock anser 20 % av de tillfrågade att de accepterar en säkerhetsrisk på 3 eller högre på den femgradiga skalan. Dock är det främst yngre som accepterar en högre risk. I allmänhet accepteras dock inte risker vid kreditkortsanvändning. Trots detta ökar kreditkortsstölder och säkerheten förbättras inte (3). När användare uttrycker risken att råka ut för bedrägeri känner användarna fortfarande oro, trots att samtliga kreditkort har chip. Endast 30 % ser risken som minimal och 28 % ser risken som liten. Detta är dock bättre än förtroendet för enbart magnetremsa. För vidare information kring fördelning längs skalan 1-5 kan läsaren vända sig till bilaga 1 i slutet av rapporten.

För att få en känsla av hur användare graderar säkerheten vid handel på Internet kontra fysisk butik samt att handla i butik mot att uthämta kontanter i bankomat, togs även detta med i undersökningen. Endast 3 % tyckte att det var säkrare att handla på Internet och detta gällde när de använde E-kort. 20 % av de tillfrågade ansåg att det inte fanns någon säkerhetsskillnad medan övriga föredrog att handla i fysisk butik. I jämförelse mellan bankomat och betalning i butik gick svaren isär. 40 % ansåg att det inte fanns någon säkerhetsskillnad medan 36 % ansåg att bankomat var säkrare, medan 24 % föredrog butik. Detta är anmärkningsvärt då skimming framförallt förekommit i bankomater och inte i butiker. Vidare är det få som vet vem som står för konsekvenserna vid kreditkortsbedrägerier. Endast 48 % anser sig veta hur förfarandet går till och vem som står för konsekvenserna. De svar som erhållits pekar dock på att färre än dessa 48 % vet vem som står för konsekvenserna då de givit felaktiga motiveringar, vilket tyder på att de inte vet svaret.

5. Analys

I resultatavsnittet presenterades att 89 % av de tillfrågade oftast eller alltid använder kreditkort vid betalning. Endast användare i åldersgruppen 46-65 år utnyttjar kreditkorts-betalning i mindre utsträckning. Dock utnyttjar huvuddelen även här kreditkortet frekvent. Svaren angående vetskapen om skimming och om skillnad i säkerhet samt teknik mellan chip och magnetremsa är relativt jämt fördelade över åldrarna. Enkäterna visar inte någon tendens att fler i en viss ålder har större vetskap än någon annan. Detsamma gäller skillnaderna mellan kunder och de som jobbar i butik. De som angivit att de vet skillnaden i teknik mellan magnetremsa och chip har ofta angivit att teknikskillnaden ligger i höjd säkerhet samt att mer information kan sparas på chip, kunskapen är därmed ytlig och det finns ingen djupare teknisk kunskap. Enkätsammanställningen tyder på att de som jobbar i butik inte har större vetskap om varken teknik eller säkerhet i jämförelse med användare och butikskunder. De ser inte heller butik som säkrare än bankomater utan huvudsakligen ser de ingen större skillnad dem emellan.

Att butik anses mycket säkrare än Internet beror på den personliga kontakten som finns vid butiksbetalning, att kortet är under uppsikt samt att det i media oftast talas om kontokortsbedrägerier över Internet. De som anser att butik är säkrare än bankomat tycker även här att den personliga kontakten är viktig samt att de anser att det är lättare att sätta olaglig utrustning på en bankomat. De som anser bankomat säkrare än betalterminal i butik gör i de flesta fall detta då de litar mer till bankernas utrustning och övervakning.

Vid medvetenhet om vem som ansvarar för konsekvenserna om kortet blir utsatt för bedrägeri är det något blandat. De flesta anger banken, medan några tror att butiken står för ersättningen och endast ett fåtal anser att de själva står för konsekvensen. Detta innebär att allmänheten anser sig vara i en säker sits om kortet blir stulet eller utsätts för bedrägeri, då de själva inte tar betalansvaret utan antingen banken eller butiken.

Anmärkningsvärt är att bland de 89 tillfrågade var det endast män som föredrog att betala kontant före kreditkort. Samtliga tillfrågade kvinnor betalade också senast med kreditkort. Däremot visar undersökningen inte på någon skillnad mellan män och kvinnor angående vetskapen om skillnaden i teknik och säkerhet mellan magnetremsa och chip. Inte heller på övriga frågor om bland annat skimming, risker och säkerhet gav något utslag mellan män och kvinnor.

Skimming har de flesta i undersökningen hört talas om och många har angivit en korrekt definition av vad det innebär. Uttryck som användning av fuskautomat, att magnetremsan läses av olagligt samt att kortet kopieras har frekvent använts för att beskriva skimming.

Anmärkningsvärt är att nyheten angående att chipfunktionen är knäckt inte tagits på större allvar av de tillfrågade i enkätundersökningen. De som sedan tidigare har vetat om det beskriver reaktionen som att de inte bryr sig, att de inte är förvånade eller att media blåst upp nyheten och att det egentligen finns väldigt liten risk som privatperson att utsättas för detta. Att det inte inneburit starkare reaktioner kan bero på att nyheten endast tog plats i media under en kortare begränsad period. Endast ett fåtal har angett negativa rektioner till nyheten.

6. Utvärdering av metod och resultat

Första utkastet av enkäten testades på fem personer vilket var av stor vikt då många av frågorna i det första utkastet var otydliga och därför missförstods. Att bland annat fyra av fem accepterade den högsta risknivån i testenkäten berodde på otydligt formulerad fråga. Enkäten

reviderades och version två anses lättare att besvara med tydligare formuleringar. Då resultatet visar att användarens allmänna uppfattning angående kreditkorts-säkerhet med magnetremsa varierar över hela skalan ett till fem kan det ifrågasättas om alla som fyllt i enkäten förstått frågan korrekt, det vill säga om frågan har formulerats tillräckligt tydligt. Resterande frågor har inte lika stor spridning vilket tyder på att det kan vara formuleringen som har skapat spridningen, inte uppfattningen hos dem som fyllt i enkäten. Dock är detta svårt att besvara utan att kontakta samtliga deltagare i enkäten igen.

I enkäten har ordet ”kreditkort” använts vilket inte har accepterats av alla som besvarat enkäten. Det har i vissa fall skapat förvirring där någon har valt att stryka ”kredit” i enkäten och någon inte förstått vilket kort som syftas till. När enkäten sammanställdes ansågs ordet ”kreditkort” användbart och de fem testenkäterna visade inte på förvirring kring begreppet, därmed har uttrycket använts även i enkätens version två. Kontokort kan vara ett bättre ord att använda då få betalar på kredit med sina betalkort.

I och med att enkäten besvarades av 89 personer där en blandning finns av ålder, kvinnor och män samt konsumenter och butiksbiträden anses enkät-undersökningen vara pålitlig samt ha en bra spridning över ålder, kön och roll. Metoden är därmed passande och väl genomförd för detta projekt.

7. Diskussion och slutsats

Allmänheten använder i stor utsträckning betalning med kreditkort och anser att användningen av dem är tillfredställande. Detta oberoende ålder, kön eller roll vid undersökningen. Kunskaperna om skillnad mellan magnetremsa och chip är begränsade, men de flesta har insikt i att chip är säkrare. Skimming är ett välkänt begrepp men att chipfunktionen skulle vara knäckt, även om detta visats på nyheterna endast för någon månad sedan, är inte utbrett bland de tillfrågade. Reaktionerna, både bland dem som uppmärksammat nyheten och de som inte visste om det sedan innan, är svagare än väntat. Att tekniken, eller säkerheten, inte är perfekt är relativt accepterat och även väntat. Några är även kritiska mot nyheter som tas upp i media och utgår ifrån att det inte ligger någon större tyngd i de påståenden som där görs.

Chip och pin är enligt Cambridgerapporten knäckt i det avseende att ett av protokollen brister. Detta innebär dock inte att ett kreditkort med chip kan utsättas för bedrägeri under en betalning i butik utan kortet måste bli stulet för att detta ska kunna utföras. Det behövs även sofistikerad teknisk utrustning och det är betydligt enklare att kopiera magnetremsan än att betala olagligt med chip i butik. Uppfattningen som de tillfrågade i denna enkät har anses därmed vara riktig och nyhetssändningen angående att chipfunktionen skulle vara knäckt har inte fått den genomslagskraft som befarats vid påbörjandet av rapporten.

Chipfunktionen är ännu inte i bruk i alla butiker trots att betalningsansvaret vid bedrägeri förflyttats till butiken om de inte installerat betalterminal som tar emot chip. Tidigare låg detta ansvar på banken eller kreditkortsutfärdaren. Att det inte alltid går att betala med chip innebär att alla kreditkort måste ha kvar magnetremsa. Vid betalning med magnetremsa i butik samt vid förlust av kort står därmed kreditkortet fortfarande inför samma risker vare sig det har chip eller inte. Det är egentligen endast vid betalningen med chip i betalterminal kunden är säkrare mot bedrägeri. I stort anser de flesta i undersökningen att det är säkert att använda kreditkort, där magnetremsa anses något osäkrare än chip. Riskacceptansen varierar något bland de tillfrågade. Trots att skimming är känt tyder undersökningen på att allmänheten inte är speciellt oroad för kreditkortsbedrägerier. Skimming kan genomföras relativt lätt men är idag inte speciellt utbrett i Sverige vilket leder till slutsatsen att de tillfrågade har en rättvisande bild av kreditkortssäkerheten.

Att de tillfrågade i undersökningen inte verkar speciellt oroad för kreditkortsbedrägerier kan ha flera orsaker. Dels är inte skimming eller andra bedrägerier så vanligt i Sverige, och dessutom tar antingen banken eller butiken ansvar för förlorade pengar vid bedrägeri, om inte kunden varit oaktsam. Detta gör att konsumenter inte sätter någon större press på butiker som fortfarande inte införskaffat chipterminaler. För att säkerheten med chip ska ha en större genomslagskraft bör alla butiker använda chipterminaler. Butikerna måste själva vilja ta ansvar för att konsumenternas betalning sker så säkert som möjligt. Då detta inte är hur verkligheten ser ut idag bör banker eller politiker sätta press på butiker att installera betalterminaler där betalning med chip kan genomföras. Detta för att skydda konsumenterna i Sverige mot kreditkortsbedrägerier i så stor utsträckning som möjligt.

Intressant är att butiksbiträden inte har en större kunskap än vanliga konsumenter, eller att konsumenterna är lika medvetna som butiksbiträdena. Intressant är även att det inte skiljer mycket mellan de olika åldersgrupperna. Detta tyder på att nyhetsflödet och informationen når till många delar av den svenska befolkningen. Då kreditkorts-bedrägerier inte är utbrett i stor utsträckning i Sverige anses den kunskap som de tillfrågade besitter fullt tillräcklig för att skydda sig mot bedrägerier.

8. Litteraturförteckning

1. *Kreditinformations hemsida.* [Online] Mars 23, 2010. http://www.kreditinformation.se.

2. *Dagens Handels hemsida.* [Online] Mars 23, 2010. http://www.dagenshandel.se/.

3. **Murdoch, Steven J., et al.** *Chip and PIN is Broken.* Cambridge, UK : University of Cambridge, 2010.

4. *Finansportalens hemsida.* [Online] Mars 23, 2010. http://www.finansportalen.se/kort.htm.

5. *School of Industrial Engineering, Purdue University hemsida.* [Online] April 8, 2010. http://cobweb.ecn.purdue.edu/~tanchoco/MHE/ADC-is/Magnetic/main.shtml.

6. *Kreditkortsinformations hemsida.* [Online] Mars 23, 2010. http://www.kreditkortinformation.se/chip-och-magnetremsa.

7. *My News Desk hemsida.* [Online] Mars 23, 2010. http://www.mynewsdesk.com/se/pressroom/cash-it/blog_post/view/ut-med-magnetremsan-cash-it-aer-emv-certifierade-484.

8. *Allt Om Spara hemsida.* [Online] Mars 23, 2010. http://www.alltomspara.se/chip-och-magnetremsa.

9. *Ny Tekniks hemsida.* [Online] April 8, 2010. http://www.nyteknik.se/nyheter/it_telekom/allmant/article46624.ece.

10. *Ge Money Banks hemsida.* [Online] Mars 23, 2010. http://www.gemoneybank.se/templates/FAQList____4328.aspx#pl_4328.

11. *Dagens Handels Hemsida.* [Online] Mars 23, 2010. http://www.dagenshandel.se/dh/DagensH.nsf/0/203A1878C86AA4D8C12576AF0034F419?open.

12. *Pan-Nordic Card authorizations hemsida.* [Online] April 8, 2010. http://pan-nordic.org/site_files/docs/press_room/1.Blad_Chip.pdf.

13. *Chip and PINs hemsida.* [Online] April 26, 2010. http://www.chipandpin.co.uk/business/card_payments/means/means.html.

14. *Swedbank ABs hemsida.* [Online] April 8, 2010. http://www.swedbank.se/sst/inf/out/infOutWww1/0,,173686,00.html.

Bilaga 1 – Användares uppfattning om säkerhet och risk vid kreditkortsanvändning

		1	2	3	4	5
Hur säkert tror ni att kreditkortet är i allmänhet? (1 låg-hög 5)	Endast magnetremsa	7 %	26 %	35 %	28 %	4 %
	Både magnetremsa och chip	2 %	0 %	27 %	57 %	13 %
Hur säkert tror ni det är att betala med kreditkort i butik? (1 låg-hög 5)	Endast magnetremsa	3 %	6 %	33 %	45 %	13 %
	Både magnetremsa och chip	6 %	3 %	12 %	53 %	26 %
Hur viktigt är det att kreditkortet är säkert att använda vid betalning i butik? (1 inte alls viktigt - mycket viktigt 5)	Endast magnetremsa	1 %	3 %	6 %	11 %	79 %
	Både magnetremsa och chip	1 %	3 %	3 %	12 %	80 %
Hur stor risk accepterar ni att kreditkortet har i allmänhet? (1 låg-hög 5)	Endast magnetremsa	53 %	20 %	17 %	6 %	3 %
	Både magnetremsa och chip	57 %	17 %	17 %	3 %	6 %
Hur stor risk accepterar ni vid betalning med kreditkort i butik? (1 låg-hög 5)	Endast magnetremsa	57 %	24 %	10 %	7 %	2 %
	Både magnetremsa och chip	63 %	18 %	10 %	7 %	2 %
Hur stor tror ni risken är för att kreditkortet råkar ut för bedrägeri? (1 låg-hög 5)	Endast magnetremsa	13 %	34 %	34 %	16 %	3 %
	Både magnetremsa och chip	30 %	28 %	26 %	15 %	1 %

Bilaga 2 – Enkät

Undersökning om allmän uppfattning om kreditkortssäkerhet

Vi är två studenter som gör ett arbete på universitetet som behandlar allmänhetens uppfattning om kortsäkerhet. Därmed skulle vi vara mycket tacksamma om Ni ville besvara de frågor som vi sammanställt i denna blankett! Att fylla i blanketten tar endast ca fem minuter av Er tid.

Vem är Ni?

Nedan följer ett par frågor som behandlar Er som person. Uppgifterna kommer att användas i syfte att göra jämförelser mellan exempelvis olika ålderskategorier.

1. Är Ni kvinna eller man?
   □ Kvinna □ Man

2. Hur gammal är Ni?
   □ 16-25 □ 26-35 □ 36-45 □ 46-65 □ 66+

3. Vilken roll har Ni vid denna undersökning?
   □ Kund □ Jobbar i butik

Betalning i butik

Här ställs några frågor kring hur Ni brukar göra Era betalningar i butik.

4. Hur föredrar Ni att betala i butik?
   □ Kontant □ Kreditkort

5. Har Ert kreditkort magnetremsa/chip?
   □ Endast magnetremsa □ Både magnetremsa och chip

6. Tycker Ni att betalning med kreditkort fungerar på ett tillfredställande sätt?
   □ Ja □ Nej

7. Hur ofta betalar Ni med kreditkort i butik?
   □ Aldrig □ Sällan □ Ibland □ Oftast □ Alltid

8. Om Ert kreditkort har chip; hur ofta sker betalning med chip av de gånger ni betalar med kreditkort?

□ Aldrig □ Sällan □ Ibland □ Oftast □ Alltid

Senaste betalning i butik

Nedan följer frågor kring hur Er senaste betalning i butik gick till.

9. Var handlade Ni senast? Ange namnet på butik, stad samt stadsdel.

Butik: Stad: Stadsdel:

10. Hur skedde Er senaste betalning i butik?
    □ Kontant □ Kreditkort

11. Om Er betalning gjordes med kreditkort; gjordes betalningen med magnetremsa eller chip?
    □ Magnetremsa □ Chip

12. Var chipfunktionen fungerande, trasig eller ännu inte i bruk?
    □ Fungerande □ Trasig □ Ännu inte i bruk

Teknik och risk

Här följer några frågor som tar upp teknik- och riskaspekter vid användandet av kreditkort. Frågorna är inte till för att testa Er som person utan för att vi ska kunna få en uppfattning om hur allmänheten uppfattar dagens kortsäkerhet.

13. Känner Ni till skillnaden i ***teknik*** mellan magnetremsa och chip på kreditkortet?
    □ Ja □ Nej
    Om ja, vilken är skillnaden? Om nej, vad tror ni skillnaden är?

Skillnad:

14. Känner Ni till skillnaden i ***säkerhet*** mellan magnetremsa och chip på kreditkortet?
    □ Ja □ Nej
    Om ja, vilken är skillnaden? Om nej, vad tror ni skillnaden är?

Skillnad:

15. Känner Ni till skillnaden mellan ***aktiva*** och ***passiva*** kreditkort?
    □ Ja □ Nej
    Om ja, vilken är skillnaden? Om nej, vad tror ni skillnaden är?

Skillnad:

16. Känner ni till vad ”***Skimming***” är?
    □ Ja □ Nej
    Om ja, vad är Skimming? Om nej, vad tror ni att Skimming är?

17. Några veckor sedan uppmärksammades i nyheterna att ***chipfunktionen är knäckt***, kände Ni till detta?
    □ Ja □ Nej
    Om ja, hur reagerade Ni på detta? Om nej, hur reagerar Ni på detta nu?

18. **Hur säkert** tror Ni att kreditkortet är i allmänhet? (Låg 1 – 5 hög)
    Kort med **endast magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Kort med **magnetremsa och chip**: □ 1 □ 2 □ 3 □ 4 □ 5

19. **Hur stor risk** accepterar Ni att kreditkortet har i allmänhet? (Låg 1 – 5 hög)
    Kort med **endast magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Kort med **magnetremsa och chip**: □ 1 □ 2 □ 3 □ 4 □ 5

20. Hur stor tror Ni **risken** är för att kreditkortet råkar ut för bedrägeri? (Låg 1 – 5 hög)
    Kort med **endast magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Kort med **magnetremsa och chip**: □ 1 □ 2 □ 3 □ 4 □ 5

21. **Hur säkert** tror Ni det är att betala med kreditkort i butik? (Låg 1 – 5 hög)
    Vid användning av **magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Vid användning av **chip**: □ 1 □ 2 □ 3 □ 4 □ 5

22. **Hur stor risk** accepterar Ni vid betalning med kreditkort i butik? (Låg 1 – 5 hög)
    Vid användning av **magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Vid användning av **chip**: □ 1 □ 2 □ 3 □ 4 □ 5

23. **Hur viktigt är det** för Er att kreditkortet är **säkert** att använda vid betalning i butik?
    (Inte viktigt alls 1 – 5 Mycket viktigt)
    Vid användning av **magnetremsa**: □ 1 □ 2 □ 3 □ 4 □ 5
    Vid användning av **chip**: □ 1 □ 2 □ 3 □ 4 □ 5

24. Anser Ni att det är säkrare att handla **med kort i butik** eller att handla med kort på **Internet**?
    □ Butik är säkrare □ Internet är säkrare □ Ingen skillnad
    Varför?
    _____

25. Anser Ni att det är säkrare att handla **med kort i butik** eller att använda kortet i **bankomat**?
    □ Butik är säkrare □ Bankomat är säkrare □ Ingen skillnad
    Varför?
    _____

Konsekvenser

26. Vet ni vem som står för ***konsekvenserna*** om Ert kort blir utsatt för bedrägeri?
    □ Ja □ Nej
    Om ja, vilka är konsekvenserna? Om nej, vilka tror ni konsekvenserna är?
    Konsekvenser:
    _____

    _____