Säkerhetsstandard för ett mjukvarubaserat säkerhetselement

SANZIDA KABIR

KTH Information and
Communication Technology

Examensarbete inom
Kommunikationssystem
Grundnivå, 15 hp
Stockholm, Sweden

Säkerhetsstandard för ett mjukvarubaserat säkerhetselement

Sanzida Kabir

2013-06-22

Kandidatexamensarbete
(Final Version)

Examinator och handledare
Professor Gerald Q. Maguire Jr.

Skolan för informations- och kommunikationsteknik (ICT)
Kungliga Tekniska Högskolan (KTH)
Stockholm, Sverige

Sammanfattning

Dagen forskare förutser att inom en snar framtid kommer majoriteten av ägarna till smarttelefon använda den som sin plånbok, det vill säga använda sig utav kontaktlös betalning. Tekniken som möjliggör kontaktklös betalning idag är närfältkommunikation (Engelska: “Near Field Communication” - NFC) som finns inbäddad i smarttelefoner. Applikationer som mobila betalningar mellan en telefon och terminal använder sig av NFC. Vid mobila betalningar sparas användarens kredit- och bankinformation och det är ytterst viktigt för en användare att dess sparade data inte kommer i fel händer. Hur ska då en användare av NFC vara säker på att säkerhetsutvecklingen går hand i hand med NFC-tekniken? Kan en användare känna sig tillräckligt säker för att spara sina privata handlingar på telefonen utan att bli bestulen?

NFC använder sig utav ett säkerhetselement (Engelska: “Secure Element” - SE) som erbjuder användaren säkerhet vid alla mobilköp men även i andra applikationer som till exempel färdmedelsbiljetter. Säkerhetselementet kommer i tre olika former: SD-kortbaserat, SIM-kortbaserat eller inbäddad i smarttelefonen. Med tiden har tekniken bakom SE vidareutvecklats och ett nytt fenomen har uppstått, nämligen ett nytt slags säkerhetselement. Den nya tekniken är ett applikationsbaserat säkerhetselement: mjukvarubaserad kortemulering (Engelska: “Software Card Emulation” - Soft-SE), som erbjuder säkerhet utan ett fysiskt SE. Denna avhandling kommer behandla säkerhetselementets område och se över om Soft-SE är så pass säker att vi kan räkna det som ett alternativ vid våra mobilköp i affären. Ett antal hot och attacker som ett SE eller allmänt en NFC-enhet kan utsättas för kommer att nämnas och en del kommer även att beskrivas samt möjliga hot och attacker mot Soft-SE. Utöver det kommer ett par för- och nackdelar med att tillämpa Soft-SE att diskuteras. Analysen är baserat på hur en användare kan få ut mer av den existerande SE istället för att tillämpa Soft-SE. Utifrån fakta, för- och nackdelar och analysen som har behandlats drogs slutsatsen att Soft-SE inte är ett säkrare alternativ än den SE som redan används av NFC-telefoner. Eftersom Soft-SE fortfarande är något nytt har den inte ännu utvecklats tillräckligt för att skydda sig mot de möjliga attacker som den kan utsättas för. Det är starkt rekommenderat att användarna av Google Wallet håller sig till det säkerhetselement som smarttelefonen använder sig utav istället för att tillämpa Soft-SE.

Nyckelord: NFC, säkerhetselement, mjukvarubaserad kortemulering, kontaktlös betalning

Abstract

Researchers today anticipate that in the near future, the majority of the owners of a smartphone will use it as a wallet, i.e. for contactless payment. The technology that enables contactless payment today is “Near Field Communication” (NFC), which is increasingly embedded in smartphones. Applications like mobile payment between a phone and a terminal use NFC. With Mobile payment the user’s credit and banking information gets saved and it’s extremely important for a user that the saved data doesn’t fall into the wrong hands. How should then a user of an NFC equipped device ensure that end-to-end security is strong enough when they use NFC technology? Can user feel safe enough to keep their private documents on the phone without getting “robbed”?

NFC uses a security element “Secure Element” (SE) that offers the user safety for their mobile purchases but also in other applications such as transportation tickets. The security element comes in three forms: SD card based, SIM card based or embedded in the smartphone. Over time, the technology behind the secure element is further developed and a new phenomenon has emerged, a new type of secure element. The new technology is an application based secure element: “Software Emulation Card” (Soft-SE), which offers security without a physical SE This thesis will deal with the Secure Element’s area to see if the Soft-SE are so confident that we can count it as an option when we do our mobile purchases in the store. A number of threats and attacks that an SE or generally an NFC device can be exposed to will be mentioned and some will also be described and some possible threats and attacks against Soft-SE. In addition, a few pros and cons of applying Soft-SE will be discussed. The analysis is based on how a user can get more out of the existing SE instead of applying the Soft-SE. Based on the facts, pros and cons, and the analysis that has been treated, it has been concluded that the Soft-SE is not a more secure alternative than the SE that is already used by NFC phones. Since Soft-SE is still new, it has not yet developed to protect themselves against the possible attacks that they may be exposed to. It is strongly recommended that users of Google Wallet adhere to the Secure Element that the smartphone use instead of applying Soft-SE.

Keywords: NFC, SE, Soft-SE, contactless payment

Innehållsförteckning

Figurförteckning

Tabellförteckning

Lista för akronymer och förkortningar

	Engelska	*Svenska*
APDU	Application Protocol Data Unit	Applikations protokolldataenheter
Google Wallet	Google Wallet	Google plånbok
NDEF	NFC Data Exchange Format	NFC datautbytes format
NFC	Near Field Communication	Närfältskommunikation
P2P	Peer-to-peer	Peer-till-peer
POS	Point of sale	Försäljningsstället
Proxy	Proxy	Ombud/fullmakt
Relay attack	Relay attack	Relä attack
RFID	Radio Frequency Identifier	Radio frekvens identifikation
SD	Secure Digital	Säker digital
SE	Secure Element	Säkerhetselement
SEEK	Secure Element Evaluation Kit	Säkerhetselements utvärderings kit
SmartCard API	SmartCard API	Smartkort API
Smartphone	Smartphone	Smarttelefon
Soft-SE	Software Card Emulation	Mjukvarubaserad kortemulering
Software-SIM	Software-SIM	Mjukvarubasead-SIM
TEE	Trusted Execution Environment	Pålitlig exekveringsmiljö
TPM	Trusted Platform Module	Pålitlig plattformsmodul
TSM	Trusted Service Manager	Pålitlig serviceansvarig
UICC	Universal Integrated Circuit Card	Universal integrerad kretskort

1 Inledning

I detta avsnitt redovisas problemområdet, syftet med studien, målgrupp, metod, samt avgränsningar jag valde att göra. Slutligen ett kort stycke om relaterande arbeten.

1.1 Problemdefinition

Det blir allt mer vanligare med närfältskommunikations[1](NFC) kompatibla smarttelefoner som lanseras som "NFC-telefoner" och är ett återkommande ämne i media idag. Vad är då NFC? NFC är ett protokoll för att kontaktlöst utbyta information över 1-10 cm korta sträckor.

Om du är ägare av en NFC-kompatibel smarttelefon[2] kan du använda den för att betala i rätt många butiker med den över hela världen. Det som möjliggör detta är applikationer som till exempel Google Wallet[1]. Enkelt, smidigt och snabbt ska det vara sägs det, men hur är det med säkerheten bakom betalningskonceptet? En av de återkommande frågorna i media är om vi ska våga lita på säkerheten bakom kommunikationen mellan två NFC-enheter med tanke på hur mycket mjukvarubaserade attacker som har utförts och som dagligen skapas för nya enheter. Kan en användare av Google Wallet som utför sina mobila köp via NFC-teknik i en butik, lita på att han/hon kan lämna butiken utan att ens privata handlingar har delats med någon obehörig via någon form av säkerhetsattack?

För en möjlig utförande av mobilbetalning via NFC krävs det ett säkerhetselement[3] (SE) som är ett krypterad och signerad chip från mobiltillverkare/leverantörer och/eller operatörer för att möjliggöra säkra mobila betalningstransaktioner[2]. Även om ett SE huvudsakligen existerar för att förse säkerhet är den i dagsläget inte helt och hållet säkert. Det har redan skett ett flertal attacker och hot direkt mot säkerhetselementet och NFC-telefoner, dessutom finns det teoretiska attacker som kommer snart att utföras i verkligheten. Finns det någon möjlighet att göra SE säkrare eller finns det ett säkrare alternativ som en användare kan utnyttja istället? Alternativet blir den mjukvarubaserade kortemuleringen[4] (Soft-SE) som är ett applikationsbaserat säkerhetselement till NFC. Frågan är om Soft-SE är redo att ta över marknaden med SE genom att tillförse mer skydd för användarna.

1.2 Syfte

Syftet med kandidatexamensuppsatsen är att få mer inblick och kunskap i ett nytt slags fenomen som kommer snarligen tillämpas i varje hem och butik samt de attacker och hot som sker och slår emot ens personliga integritet. Mitt bidrag till information blir således i form av ett konkret exempel om operatörlösa Soft-SE kan öka säkerheten för kontaktlösa mobilbetalningar och NFC-enheter.

1.3 Målgrupp

Denna avhandling är främst avsedd för studenter inom Informations- och kommunikationsteknik, min handledare, och mig själv. Det är även för alla andra som vill ha en överblick på säkerheten för framtida användande av NFC samt de som vill ha mer kunskap om det alternativa säkerhetselementen som har introducerats av NFC.

---

[1]Engelska: "Near Field Communication"
[2]Engelska: "Smartphone"
[3] Engelska: "Secure Element"
[4]Engelska: "Software card emulation"

1.4 Metod

För att finna en lämplig säkerhetsstandard hos både interna/externa SE och Soft-SE kommer jag att gå igenom lämpliga attacker som har skett hos SE och som kan utgöra hot för Soft-SE. Förutom de valda attackerna, diskuteras säkerhetselementets säkerhetsstandard ur andras perspektiv som har utfört dessa attacker. Val av attacker gjordes beroende på hur pass populära de var bland författarna som diskuterar eller har utfört dessa attacker. Fördelar och nackdelar för respektive SE kommer även att diskuteras innan det slutgiltigta slutsatsen dras ifall Soft-SE är lika pass säker som de existerande SE:n som erbjuds.

Alla ingående delar i de säkerhetselement som diskuteras förutsätts vara säkra och osäkra ur någon synpunkt. Utifrån litteratur kring NFC och SE, rapporter, rekommendationer, avhandlingar och artiklar är dessa säkerhetsattacker och hot diskuterade.

1.5 Avgränsningar

För detta arbete kommer fokus ligga på säkerhetselementen som har introducerats inom NFC-teknik, det vill säga SE och Soft-SE. Soft-SE är fortfarande en ny slags strategi som har introducerats och är fortfarande på utvecklingsstadiet, därför kommer materialet som används vara från 2011 och uppåt. Då säkerhetsstandarden varierar från attack till attack kommer ett fåtal lämpliga fall väljas ut för jämförelse samt diskussion. Likadant med för- och nackdelar som kommer att avgränsas till ett fåtal till Soft-SE.

1.6 Relaterande arbeten

En hel del arbeten, avhandlingar, artiklar och rapporter kan finnas för både NFC och SE. Däremot är det fåtal som finns ute för Soft-SE eftersom det fortfarande är så pass ny och har inte testats lika mycket av NFC- tekniker.

Michael Roland täcker den beskrivande delen av Soft-SE väldigt bra och kommer användas som en flitig referens för denna avhandling. För övriga relaterande arbeten om hot och attacker är *A Practical Relay Attack on ISO 14443 Proximity Cards* av Hancke[3], *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones* av Francis et al.[4] och *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* av Kfir och Wool[5].

2 Mobila betalningar

Mobil betalning är en komposit betalningsmodell som omfattas av olika paradigm där alla kännetecknas från användningen av mobila betalningar. Huvudtypen av denna betalningsmodell är näransluten betalning.

En av de primära tjänsterna för näransluten betalning är kontaktlös betalning som baseras på standardiserad teknologi genom en trådlös förbindelse med kort räckvidd, med andra ord NFC, där NFC-telefonen kännetecknas som ett ”mobilt plånbok”. Kontaktlös betalning sker genom att en smarttelefon med ett NFC – chip (som sänder data) förs nära en NFC aktiverad terminal[1] (POS) på försäljningsstället med en räckvidd på högst 4 centimeter eller mindre[6] mellan enheterna (se Figur 1). Betalaningen sker inom några få sekunder.

Figur 1: Kommunikation mellan smarttelefon och POS-terminal

Med innovativa betalningssätt kommer det säkerhetsrisker som användaren måste vara medveten om (Tabell 1). Bedrägeri på mobiltelefoner är inte ett nytt ämne och dagens mobilsäkerhet reflekterar industrins upplevelse att strida mot bedrägerier. Mobilenheter finns nästan hos varje individ och är nästan alltid påsatt, vilket gör att säkerhetsperimetern blir bredare, det vill säga bedrägeririsken ökar.

Tabell 1: *Säkerhetsrisker*

Mobila betalningsrisker:
Transaktionsbedrägeri
Plattformssäkerhet
Hot i applikationsdatabas
SIM-kort applikationsattacker
Säkerhetsrisker i applikationsbutik
IP-baserade applikationshot
Mobiltelefoni säkerhetsrisker

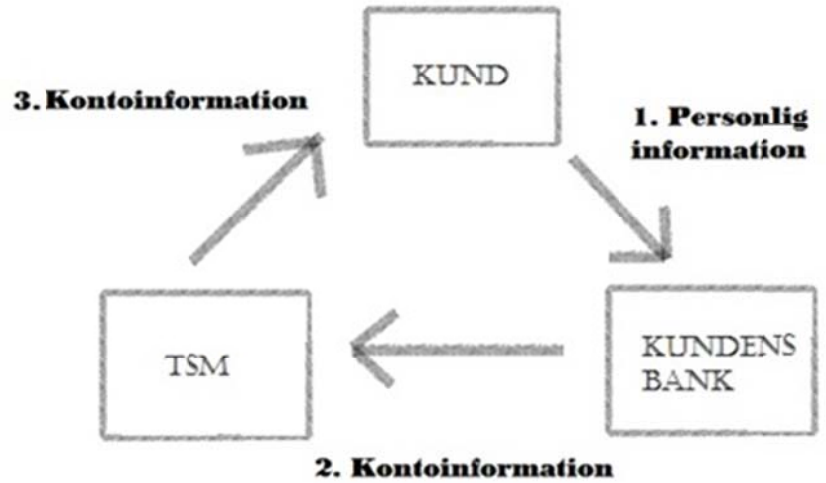
[1] Engelska: ”Point of Sales”

2.1 POS terminal

Ett NFC POS terminal är en NFC– aktiverad elektronisk betalterminal[7] som kan anslutas till de flesta smarttelefonerna[8] och genomföra samt validera en betalning via mobiltelefonen. Denna NFC POS terminal ersätter den traditionella kassaapparaten.

2.2 Google Wallet

Google Wallet är en betaltjänst för smarttelefoner - ett system för betalkort med inbyggd radiofrekvens identifikation[1] (RFID) teknik för trådlös kommunikation[9] som installeras i en NFC-kompatibel mobil. Vid betalning skickas bankkortsinformationen som finns lagrad i ett inbäddat SE till POS terminalen via NFC. En betalning sker endast när applikationen är öppen och användaren har tryckt in sin 4-siffriga pinkod. Google Wallet sänder då informationen till flera säkerhetskanaler för verifikation (*se Figur 2*)[10]. Kundens personliga information går igenom den första kanalen till kundens bank som vidare skickar kundens kontoinformation genom den andra kanalen till en pålitlig serviceansvarige för en ytterligare verifikation, slutligen vidarebefordras kontoinformationen till kunden och ett lyckat köp har utförts.



Figur 2: Googles kontaktlösa informationsöverföring via TSM(se kapitel 4)

Cynagenmod som en relativ ny mjukvara för Android-telefoner, som möjliggör en Google Wallet användare att välja inbäddad SE eller det nya alternativet Soft-SE för säkra köp[11]. För att Google Wallet ska kunna använda Soft-SE krävs det en smarttelefon som stödjer kortemulering, dvs. tillåta NFC-enheten att fungera som ett kort, i det här fallet ett betalkort. Kortemulering stöds av alla kontaktlösa terminaler, där NFC-enheterna visas som en kontaktlösa smartkort för läsaren. Google Wallet förlitar sig då på kortemulering för överföringen av autentiseringsuppgifter till POS-terminalen[12].

2.3 Cynagenmod

Cynagenmod är en ersättande firmware för en rad smarttelefoner baserad på Android operativsystemets öppna källkod[32]. Den erbjuder en rad inslag som inte finns i Android baserade firmware av leverantören av dessa mobiltelefoner. Denna firmware har så kallade

[1]Engelska: ”Radio Frequency Identifier ”

”patchar” för att aktivera kortemulering på telefonen med NXP's NFC chipset[1] [13]. NXP är ett företag inom halvledarindustrin som erbjuder standardlösningar baserat på bland annat radiofrekvenser.

[1]Kallas även för PN544

3 Närfältskommunikation

Närfältskommunikation eller NFC är en kontaktlös kommunikationsteknologi som baseras på RFID tekniken (ISO/IEC 14443) och har godkänts som en standard av både ISO/IEC (ISO/IEC 18092, ISO/IEC 21481) samt ECMA (ECMA- 340, ECMA-352)[14]. Denna standard definierar bland annat att data överförs på frekvensbandet 13,56 MHz, att tekniken är kompatibel med RFID samt en Japansk RFID smartcard teknik skapad av Sony. Förutom vad som definieras utav standarderna ISO/IEC och ECMA, har ett forum kallat NFC-Forum[15] över specifikationerna på bland annat olika dataformat, protokoll, certifiering.

När två NFC-enheter kommer i kontakt med varandra aktiveras omedelbart en åtgärd. För att en sådan åtgärd ska aktiveras krävs NFC Data Exchange Format(NDEF) som är en definierad standard av NFC Forum och används för att två enheter skall kunna kommunicera med varandra. NFC-enheter kan kommunicera med både aktiva taggar och passiva RFID-taggar. Skillnaden är att aktiva taggar har en egen strömkälla för att skicka ut signaler till läsaren medan passiva taggar använder sig utav det elektromagnetiska fält som läsaren skickar ut. Dessa taggar kan innehålla allt ifrån kreditkortsnummer, personlig information till meddelanden, och koder.

Figur 3: En NFC-telefon har en rad olika funktioner. En användare kan betala sina köp via POS-terminal, dela företagskort, använda telefonen som färdmedel i tåg och buss, skriva direkt ut från kameran genom att vinka telefonen framför skrivare och få information från smarta affischer.

Det finns tre olika åtgärdsoperationer: läsa/skriva[1] läge, icke-hierarkiskt nät[2] (P2P) läge, och kortemulerings läge. På läsa/skriva läget kan NFC-enheter få tillgång till kontaktlösa smartkort, NFC-taggar, och RFID transponder. På P2P läget kan två NFC-enheter kommunicera direkt med varandra. Vid kortemulerings läge, emulerar en NFC-enhet en kontaktlös smartkort, det gör att den kommunicerar med existerande RFID läsare.

År 2012, utvecklades en öppen källkods Java bibiliotek av Antonio Loltito; som implementerade NFC Forums ‟Simple NDEF Exchange Protocol” (SNEP) som tillåter P2P mellan olika NFC-enheter[16]. Tidigare användes ett annat protokoll, ‟NDEF Push Protocol” (NPP) som utvecklades av Google och är endast tillgängligt på Android-enheter. SNEP däremot är den officiella specifikationen av NFC Forum för P2P.

Det finns ett flertal vägar för NFC-data att gå genom chipsetet i en NFC-telefon. Applikationsprocessorn är NFC-telefonens främsta behandlingsenhet. NFC-kontroller är kärnkomponenten av NFC:s funktionalitet i en enhet som innehåller NFC-modem och utför

[1]Engelska:”Read/write”
[2]Engelska: ”Peer-to-peer”

förbehandling av kommandon och data. SE är ett smartkorts mikrochip som kan utföra säkra kortemulering. P2P läge, läsare/skrivare läge, och Soft-SE tar rutten mellan applikationsprocessorn och NFC-interface med kommandon och data. NFC-interface är sammansatt av kontaktlös analog-till-digitalt på främre änden av en NFC-enhet[17]. Säker kortemulering använder rutten mellan säkerhetselementet och NFC-interface. Förutom den externa åtkomsten genom NFC-interface är SE:n ansluten till applikationsprocessorn, vilket gör att innehållet i SE kan hanteras inifrån mobiltelefonen och genom mobilnät[18]. SE kan antingen ansluta till applikationsprocessorn direkt eller genom NFC-kontrollen.

3.1 NFC Protokoller

NFC är en uppsättning av kommunikationsprotokoller baserat på RFID standarden. I protokoll lagret sker själva överföringen av data som är avsett till att skickas eller mottas under kommunikationen[19]. Det finns en mängd olika protokoller i NFC-enheter men i denna avhandling är det enbart protokollet typ 4 tagg[20] som kommer att nämnas.

Cruz[21] presenterade protokollet Mtrocos för att genomföra mobila betalningar, som besitter ett antal karaktäristiska drag såsom, anonymitet, hög säkerhet, stöd för mikrobetalningar och inga speciella hårdvarukrav. Designen är baserat på digitala pengar samt *ad hoc* nyckel etablering. Ett annat protokoll som kan vara användbar för att läsa sig om underliggande kommunikationsprotokoll är NFCProxy. Lee[22] från Blackwingintelligence visade hur det är möjligt att proxy[1] transaktioner mellan en RFID kreditkort och en läsare. Den sparade transaktionen kan återspelas för smygkopiering av kreditkort eller kan RFID kreditkortet återspelas vid POS-terminalen. För att möjliggöra en återspelning vid läsaren måste enheten ha CyanogenMod.

3.2 Genomförda attacker

I denna del kommer ytterligare en del hot och attacker inom NFC att introduceras som har genomförts av andra. Djupare beskrivning av olika slags vanliga attacker på säkerhetselementen finns under sektion 6.

Ju mer NFC blommar ut i marknaden desto fler attacker utförs det av olika slag. Här är några exempel på möjliga attacker och hot som en NFC-användare kan råka utför:

- ***Identitetsstöld***
- ***Lösenordsfiske***
- ***Skimning av transaktioner***
- ***Övervaka PIN-kod***
- ***Avlyssning av varor***
- ***Injicera skadlig kod/innehåll***

Mulliner[23] har presenterat ett flertal NFC-attacker på NinjaCon/B-sides Conference i Vienna. Boingboingtv har lagt upp ett klipp på Youtube där man få se hackaren Holman[24] visar hur man dekrypterar en RFID-kompatibel kreditkort via en läsare som han köpte från eBay. Läsaren som är kopplad till en dator visar all kreditinformation som hackaren enkelt kan använda sig av för att gå online och börja köpa. Koden borde dekrypteras i banken och inte vid köp. Miller [25] visade att genom att köra en skadlig kod i en NFC-telefon kan den

[1] Server som agerar mellanhand för förfrågningar från klienter som söker resurser från andra servrar.

göra den till en botnet zombie[1] eller hämta känslig information. Experter från *The Intrepdius Group*[26] har utvecklat en Android applikation till NFC-telefon, som kan kopiera data från en helt ny tågbiljett och skriva tillbaka till kortet när antalet resor tar slut.

3.3 Kortemulering

Det existerar flera möjliga alternativ för NFC kortemulerings läge. Emuleringen kan skilja i kommunikations standard, i kompatibla protokollskikt, i kompatibla kommando set och i den del av NFC enhet som utför själva emuleringen. Kortemulering representerar routing kommunikationen från en extern kontaktlös terminalläsare till det inbäddade SE där endast SE och NFC-kontrollen är involverade.

Det finns tre olika kommunikationsstandarder: ISO/IEC 14443 Type A, ISO/IEC 14443 Type B och FeliCa (JIS X 6319-4)[18]. Support för dessa lägen beror på NFC-kontrollen, SE och den geografiska regionen.

En annan skillnad är den del av enheten som utför själva emuleringen. En kort kan emuleras i en mjukvara[2] eller utföras av det hängivna SE.

[1] Någon utomstående som har tagit kontroll över enheten och som använder den till att utföra uppgifter som säkerhetsattacker.
[2] På enhetens applikationsprocessor.

4 Säkerhetselement

SE är en exekveringsmiljö[27] där applikationskoder samt applikationsdata kan lagras i säkerhet, administreras, och utföra säker exekvering av applikationerna. SE innehåller avgränsat minne för varje applikation och andra funktioner som kan kryptera, dekryptera, och signera datapaketet[27]. SE kan komma i olika former för att bidra med säkerhet till en NFC-enhet.

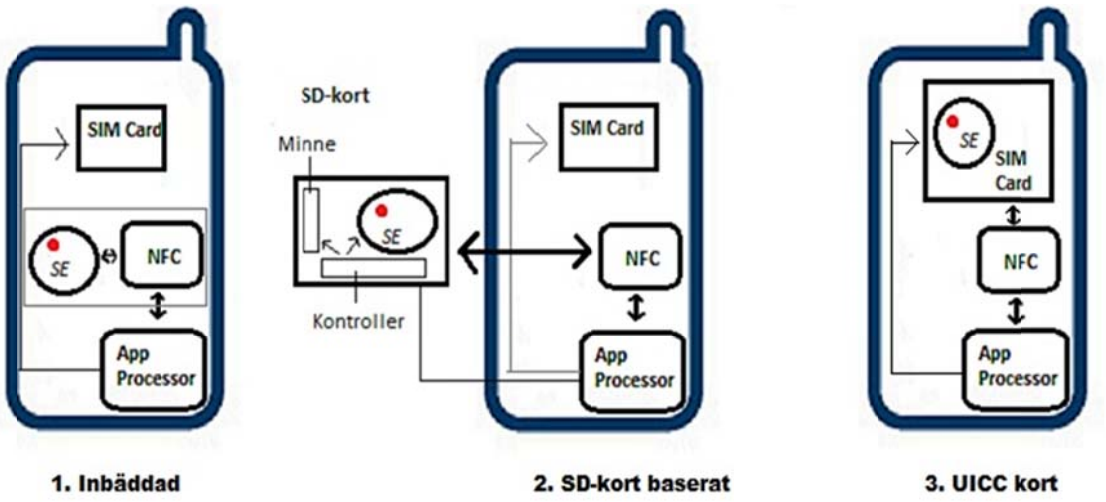
De tre vanligaste formen av SE: inbäddad SE[1], SE på UICC (SIM), och SE på minne.

- Inbäddad SE, en säkerhetskomponent som är inbäddad i en NFC-enhet och kan lagra och hantera affärs-och personlig information på ett säkert sätt. Denna särskilda smartkort chipset är inbäddad i enheten vid tillverkningen.

- Smartkort för mobilterminaler i GSM- och UMTS-nät[2](UICC), en generisk och väl standardiserad, fysiskt och logisk plattform för smartkortsapplikationerna. UICC är vanligtvis utfärdad av en part som vanligtvis har minst en applikation på kortet. UICC kort används av mobilnätoperatörer som inkluderar en USIM (UMTS/3G SIM) applikation på kortet för att verifiera användaren i ett 3G-nät[28].

- Mikro SD-kort, ett minneskort med ett inbäddat chip som används som ett SE. Det finns SD produkter som både innehåller och inte innehåller NFC antenn.

Vilken form av SE som ska implementeras i en NFC-telefon bestäms av respektive mobilleverantör och/eller betaltjänstleverantören[27].



Figur 4: De tre olika säkerhetselementen som används i NFC-telefoner.

En nackdel är att betalningsapplikationerna är begränsade till SE:s kapacitet, tillgång till SE är slöare, autentiseringsuppgifter för inbetalning är en komplex och skör process som inkluderar flera pålitlig serviceansvarig[3], flera leverantörer och flera SE och enheter[12]. Det är här Soft-SE kommer in i bilden med andra och möjligtvis förbättrade preferenser.

[1]Utanpåliggande smartkortschip
[2]Engelska: "Universal Integrated Circuit Card"
[3]Engelska: Trusted Service Manager - TSM

I dagsläget är alla SE hårt kontrollerade av leverantörer och mobiloperatörer. Det gör att vem som helst inte kan skapa en applikation utan att ha tillgång till SE för att installera applikationen. För att få tillgång till sitt SE i telefonen, måste användaren få tillgång till "nycklar" för att komma åt elementet. "Nycklarna" finns hos leverantören/operatören och det är ytterst sällan de ger upp dessa nycklar för utveckling till en användare, såvida det inte är en tjänsteleverantör som kanske gör en storsatsning på en applikation. TSM har en viktig roll inom NFC:s ekosystem. Det är TSM som sätter upp affärsavtal och tekniska förbindelser med mobiloperatörer, mobiltelefontillverkare, och andra inblandade företag som styr SE på NFC-telefoner. TSM möjliggör för tjänsteleverantörer att distribuera och hantera sina beröringsfria applikationer på distans genom att tillåta åtkomst till SE.

5 Mjukvarubaserat säkerhetselement

År 2011 släppte Research In Motion (RIM)[1][29] ett nytt tillvägagångssätt till kortemulering i NFC-kompatibla mobiltelefoner på deras BlackBerry plattform så kallad Software Card Emulation eller "Soft-SE"[2]. Utöver introduceringen av support för olika säkerhetselement, presenterade Blackberry 7 även support för emulering av NFC-tagg och smartkortläsare genom mjukvara på deras mobiltelefons applikations processor[30].

Applikationen i mobiltelefonen kan emulera en NFC Forum typ 4 tagg genom enkelt specificera en NDEF meddelande som skall vara lagrad i den virtuella taggen. Typ 4 taggens protokoll hanteras automatiskt av BlackBerry system. Detta kan användas till att utbyta data med en annan NFC-enhet som funkar i läsa/skriva läge.

ISO/IEC 14443-4 smartkortläsare kan också emuleras av en applikation. Både för ISO/IEC 14443 Typ A och Typ B protokoll varianter är emuleringen möjlig. En applikation kan specificera statiska egenskaper av den emulerade smartkorts läsare och kan utbyta protokolldataenheter på toppen av blockets överföringsprotokoll som definieras av ISO/IEC 14443-4[11]. När en applikation vill agera som ett kontaktlöst smartkortsläsare, registrerar den sig med Blackberry systemet. När ett kommando tas emot från en extern RFID/NFC-läsare, utförs en callbackmetod. Kommandot som mottas, skickas som en parameter till callbackmetoden. Applikationen kan då behandla kommandot och leverera ett returvärde som ska returneras till läsaren[18].

Förutom RIM i Blackberrys telefoner finns det Cynagenmod som nämndes tidigare, som stödjer Soft-SE i Androidtelefoner[18]. När exempelvis en Cynagenmod implementerad telefon startar Google Wallet får användaren välja om applikationen ska startas i den inbäddade SE eller i Soft-SE[31]. När en betalning sker via Google Wallet i en butik registrerar POS-terminalen Soft-SE som ett kontaktlös kort. Data från Soft-SE presenteras i samma format som används i standard kortemuleringsläge för transaktioner[32].

Soft-SE skiljer sig från de reguljära SE genom att istället för att routing kommunikationen mottas av NFC-controller till SE, överförs kommunikationen till NFC:s serviceansvarige som kommer tillåta kommandon behandlas av applikationer som finns installerade i NFC-telefonen. Med denna metod bryts beroendet av SE:n genom att tillåta autentiseringsuppgifterna lagras någon annanstans - i applikationsminnet, pålitlig exekveringsmiljö[3](TEE), eller på molnet.

5.1 Fördelar och nackdelar

Här presenteras för- och nackdelar med Soft-SE likställt med den reguljära SE.

I dagsläget finns det många existerande betalnings-, biljetthanterings och passeringskontroller som har stationära infrastrukturläsare som endast användare med mobiltelefoner som stödjer kortemulering kan ta del av. Med kortemulering kommer användaren att använda mobilen som smartkort/kontaktlösa polletter. Trots det, är kortemulering och säkerhetselementet en komplicerad terräng som inte vem som helst kan ta del av. Inbäddade SE är vanligtvis kontrollerad av enhetstillverkarna eller TSM. UICC som SE är kontrollerad av mobiloperatörer. För den som vill ha tillgång till sitt säkerhetselement,

[1] RIM är nu känd som Blackberry.
[2] Kan refereras som "Host card emulation" – HCE
[3] Engelska: Trusted Execution Environment

finns det tre barriärer som måste gås igenom. Den första barriären blir de olika partierna som driver säkerhetselementen. Den andra barriären kommer vara att operaören som redan ger en viss service kommer att tillåta sina tävlingskompanjoners liknande service på deras SE. Den tredje barriären blir kostnaden att få en applikation i säkerhetselementet. Förutom hyreskostnaden för utrymme i säkerhetselementet, måste applikationerna ha en form av säkerhetscertifikat om de ska samexistera med andra applikationer i en och samma SE. Dessa tre barriärer gäller alla utvecklare förutom de stora organisationerna och betalsektor som vill få in deras applikationer i telefonen. Lösningen till utvecklarnas problem är säkerhetselement i form av Soft-SE i NFC-telefoner. Med Soft-SE kan vilken utvecklare som helst skapa applikationer i kortemulerings läge utan att ha tillgång till säkerhetselementet. Detta öppnar utveckling av applikationsbasering på existerande stationära infrastrukturläsare. Utvecklarna kan med Soft-SE, skapa applikationer, där RFID biljetter och smartkort redan används, såsom accesskotroll, betalning, transporteringsbiljetter.

Det finns enheter ute på marknaden som inte stödjer P2P-läge men däremot finns det system som är baserade på NPP och SNEP som endast kan utbyta ett meddelande i en riktning varje gång två NFC-telefoner nuddar varandra[18]. Soft-SE kan användas som ett alternativ för P2P läget för kommunikation mellan två NFC-enheter. Det är många existerande kontaktlösa smartkortsläsare vars PC plattformar inte har support för P2P, då är soft-SE ett alternativ. Det är en enkel interaktion mellan mobiltelefonen och PC systemet utan några extra kostnader för en ytterligare NFC hårdvara.

Alla dessa fördelar kommer tyvärr med en rad nackdelar också. Förutom tekniska begränsningar i Soft-SE är det även signifikanta säkerhetsbrister. Om inte applikationsprocessorn själv tillför någon form av pålitlig datorteknologi(vilket nuvarande mobiltelefoner inte gör), exekverar applikationen på mobiltelefonens applikationsprocessor och drar ingen nytta alls av säkerhetsdatalagringen och TEE av säkerhetselementet.

Utan säkerhetslagring blir det svårt för kortemulerings applikationer att spara känslig data som till exempel kreditinformation och information för accesskontroll. Brist på pålitlig exekveringsmiljö kan leda till avsiktliga störningar av andra applikationer. Beroende på hur känslig data en användare har kommer vissa ändå ta risken och använda Soft-SE. Å ena sidan, kan det vara värt risken om det handlar om enstaka färdbiljetter eller eventbiljetter, då risken för att bli utsatt för oväntade attacker är liten. Å andra sidan, borde användaren ta den säkra vägen och använda sig utav de reguljära säkerhetselementen när det handlar om kreditinformation och accesskontroll. Kreditkort och nycklar som är sparade i mobiltelefonen är alltför känslig data som kan bli skimmade.

Den Soft-SE som finns i Blackberrys och telefoner med Cynagenmod, stödjer endast emulering av ISO/IEC 14443-4 smartkort. Det betyder att egenutvecklade system som fungerar på det lägre protokolletlagret inte kan emuleras. Soft-SE är inte användbar för flera äldre RFID system[18]. Slutligen, de mobiltelefoner som genomgår emulering en gång kan inte återuppta det säkerhetselement som användes innan emuleringen.

6 Hot och Säkerhet

I detta avsnitt beskrivs en rad attackscenarion för både externa och interna SE. Jag börjar med en beskrivande del om reläattack som är den vanligaste attackformen inom NFC och utgör en stor hot mot SE. Därefter nämns några andra vanliga attackformer och slutligen hot och attacker som Soft-SE kan drabbas av.

6.1 Reläattack

Denna form av attack har uppmärksammats ytterst i kreditkortstransaktioner. Reläattack[1] innebär en attack på överföring mellan två kanaler. Vid den vanligaste reläattacken överförs meddelanden från ett läge till ett annat för att få en enhet att verka befinna sig närmarare än vad den egentligen är[33]. En lyckad utförd reläattack kräver tre komponenter[34]:

- En läsarenhet närheten av kortet under attacken. Med en annan benämning kallas det ofta för ”mullvad[2]” eller ”igel[3]”.
- En enhet till kortemulator som används för att kommunicera med den verkliga läsaren. Kallas ofta för “proxy”[3] eller ”spöke[4]”.
- En snabb kommunikations kanal mellan enheterna[26].

Hancke[3] är bland de första som bevisade en reläattack på signaleringslagrets kommunikation mellan ett smartkort och RFID-läsare. Möjligheten att förbättra kommunikationsdistansen mellan enheterna och enklare komma åt offrets smartkort bevisades av Kfir och Wool[5]. Nyligen visade Roland, Langer, och Scharinger[35] att reläattack kan utföras genom mjukvaran av mobilens applikations processor. Francis et al.[4][36] visade att en reläattack kan utföras via Bluetooth™ och trådlösa kommunikationskanaler i NFC P2P läge och kontaktlöst smartkorts kommunikation.

Flera metoder har skapats för att förhindra reläattacker utan att lyckats. Det nuvarande kryptiska protokollet på applikationslagret kan inte förhindra dessa attacker. Exempel på metoder som har skapats för att skydda enheten är pinkod och/eller lösenord som används för tvåfaktorsautentisering, skydd som aluminiumfolie till kortets radiofrekvenser när den inte används och protokoller för att bestämma det verkliga avståndet mellan kortet och läsaren.

6.2 Andra hot och attacker

Här presenteras andra form av hot och attacker som kan ske när två NFC-telefoner kommunicerar.

6.2.1 Tjuvlyssning

När två enheter kommunicerar med varandra via NFC använder de sig utav radiovågor för att prata med varandra. En attackerare kan använda sig utav en antenn för att motta transmitterande signaler och extrahera samt tolka informationen i radiovågorna. Dock är det inte fastställt vilket avstånd som krävs för en lyckad attack av tjuvlyssning.

[1] Engelska: ”Relay attack”
[2] Engelska: “Mole[3]”
[3] Engelska: “Leech”[5]
[4] Engelska: “Ghost”[6]

Det finns inget bra sätt att skydda sig mot tjuvlyssning inom NFC men om data sänds i ett passivt läge är det svårare att tjuvlyssna för attackeraren. Passivt läge är dock inte tillräckligt för applikationer som sänder känslig data. Alternativet är att upprätthålla en säker kanal mellan två NFC-enheter med hjälp av ett standardiserat krypteringsprotokoll[37].

6.2.2 Data korruption

En attackerare kan även modifiera den data som transmitteras via NFC-interface. Attackeraren kan störa kommunikationen så att mottagaren inte förstår den data som sänts från andra enheter. Data korruption kan åstadkommas genom att transmittera giltiga frekvenser av dataspektrum under rätt tidpunkt.

NFC-enheter kan motverka data korruption genom att kontrollera radiovågornas fält medan data transmitteras[37]. På det sättet kommer enheterna att upptäcka attackerna.

6.2.3 Data modifikation

Denna attack skiljer sig från data korruptionen. Här vill attackeraren att den mottagande enheten faktiskt mottar giltig men modifierad data. Genomförbarheten av detta angrepp beror i hög grad på den tillämpade styrkan av amplitudsmoduleringen[37].

Användaren kan skydda sig mot data modifikation genom att aktivera aktivt läge hos båda parterna vilket gör det omöjligt för attackeraren att modifiera all data som transmitteras via radiovågornas länk. Däremot är detta skyddsätt sårbar på andra sätt vilket gör att alternativa skyddsätter är att föredra. NFC-enheter kan kontrollera radiovågorna vid sändning och stoppa data transmissionen vid upptäckt av attacker. Det sista alternativet att skydda sig mot data modifikation är via säkra kanaler.

6.2.4 MITM-attack

I en MITM-attack[1] finns det en tredje person (Trudy) när två personer (Alice och Bob) kommunicerar. Den information som skickas mellan Alice och Bob ses även av Trudy. Alice och Bob har ingen uppfattning om att de inte skickar och tar emot data till och från varandra men båda sänder och tar emot data från Trudy. 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.

6.3 Möjliga hot och attacker på Soft-SE

Som det nämndes tidigare är Soft-SE ett alternativt säkerhetselement för Google Wallet. Hoog[38] och Rubin[39] har skrivit att Google Wallet tillåter obehöriga att ta del av kreditinformationen samt PIN-koden till plånboken eftersom även om Google Wallet har tillgång till ett SE i telefonen är dess data cachad inom applikationens privata datalaagring i mobiltelefonens minne.

Vid användning av Soft-SE sparas ett ”virtuellt kort” på en avlägsen plats och använder mobiltelefonen som en proxy för att komma åt det virtuella kortet. Kommandon från POS-terminalen vidarebefordras då till det virtuella kreditkortet som lagras på en fjärrserver. Svaret som tas emot från det virtuella kreditkort dirigeras tillbaka till POS-terminalen. Tillgång till detta virtuella kreditkort måste säkras mot kapning[2] av pågående kommunikation samt mot obehöriga från att använda kreditkortet genom krypterad och autentiserad tunnel och genom att lösenordet inmatas av användaren före användning. Med tanke på att många av nuvarande

[1] Engelska: ”Man in the middle”
[2] Engelska: ”Hijack”

mobiltelefoner utsätts för attacker som tillåter hämtning och hantering av privat information som finns lagrade i applikationer, måste en säkerhetstunnel skapas som inte kan ”hijackas” av andra applikationer[18]. Dock är det en utmanad uppgift att skapa en säkerhetstunnel. Förutom säkerhetsriskerna, krävs det en stabil internetuppkoppling under hela transaktionen för att inte störa, förlänga eller avbryta en transaktion.

Sårbarhet av dataanvändning för Soft-SE är inte de enda säkerhetsriskerna. En annan säkerhetsfråga som har fått en ökad betydelse på grund av Soft-SE är användingen av mobiltelefoner som attacksplattform. Som det nämndes tidigare visade Francis et al.[36] att NFC-telefoner kan användas för att utföra reläattack vid kommunikation på P2P läget över längre distans. Likande attacker kan utföras med kontaktlösa smartkort[3][5]. En mobiltelefon som stödjer Soft-SE har den ideala formfaktorn och varierande nätverksgränssnitt för att etablera en reläkanal. Kontaktlösa smartkort kan enkelt utföras för relä genom två NFC-telefoner[4]. Den ena telefonen i läsa/skriva läge som beter sig som proxy mellan smartkorten och reläkanalen. Den andra telefonen i Soft-SE läge som beter sig som proxy mellan reläkanalen och RFID/NFC-läsaren (t.ex. POS-terminal). Roland et al. har demonstrerat att ren mjukvara på offrets mobiltelefon är tillräcklig för att utföra proxy på kommunikationen mellan SE och reläkanalen.

7 Analys

Säkerhetselementet tillförs i NFC-telefoner just för att ge användaren säkerhet i olika applikationer och skydda dess data. Trots alla hot och attacker som har utförts är säkerheten hög nog för att skapa tillit bland tillverkare/operatörer/leverantörer som erbjuder dess säkerhet i form av tre element till sina kunder samtidigt som de har makten över de och inte låter vem som helst ta del av elementen för att till exempel skapa applikationer. Många kritiker hävdar att om man har utfört kortemulering en gång på sina telefoner, kan användaren inte längre lita på SE där kommunikationen hanteras av mjukvara på applikationsprocessorn. Detta är en risk som en användare får ta vid användning av Soft-SE. Däremot har användaren fria tyglar och blir ägare av sitt egna element med inga andra mellanhänder. Enligt Michael Roland[40] som har gjort en hel del forskning om Soft-SE, är det troligtvis inte möjligt att få en bättre säkerhet än SE med nuvarande mobilarkitektur. Däremot, genom att använda pålitliga plattformar[1] kan man nå tillräckligt mycket säkerhet för många applikationer. Alternativ på emulering är Software-Sim som emulerar Sim-kort och gör betalda applikationer åtkomliga. Ett annat sätt att kommunicera med SE utan att implementera Soft-SE, är med hjälp av Secure Element Evalution Kit(SEEK) som även kallas för SmartCard API för Android plattformar.

7.1 Pålitliga plattformar

Ett sätt att utöka sin säkerhet på den UICC-, inbäddade- och SD-kort baserade säkerhetselement är att tillämpa pålitlig plattformsmodul[2] (TPM) eller ARM TrustZone. Ekberg, Konstiainen et al från Nokia Research[41] har flera publikationer på både TPM och ARM TrustZone.

TPM är en specifikation som beskriver en säker kryptoprocessor som kan lagra kryptoriska nycklar som skyddar informationen. Programvaran kan använda TPM för att autentisera hårdvaruenheter. Varje TPM-chip har en unik och hemlig RSA nyckel som brändes in när chippet producerades, därför är den kapabel till att utföra autentisering av plattformen. TPM minskar risken att data kommer kompromettеras av fysisk stöld eller attacker av en extern hacker. Skyddet på hårdvaran är i sig mindre utsatt för mjukvarubaserade attacker och autentisering utförs genom ett säkert delsystem[42].

ARM TrustZone är ett omfattande systemstrategi för dataplattformar med hög prestanda för applikationer som kräver säker betalningssystem. Med systemet är det möjligt att säkra kringutrustningen som säker minne, kryptoblock, tangentbord och skärm för att säkerhetsställa att de kan skyddas från mjukvaruattacker[43]. TrustZones teknikbaserade systemchip som kör en TEE skild från den huvudsakliga OS, skyddar pålitliga applikationer från mjukvaruattackar och skadliga program. TrustZone växlar till ett säkert läge och ger hårdvarustödda isolering. Pålitliga applikationer tillåter applikationer från olika betalningsföretag/banker att samexistera på en och samma enhet[43].

7.2 Software-SIM

Förutom emulering av SE, finns det en applikation så kallad Marker Access som emulerar ett SIM-kort(Software-SIM) från en valfri operatör och gör betalda applikationer åtkomliga på Android Marknaden[44]. Detta slags emulering utförs oftast av Android- användare som vill

[1]Engelska: ”Trusted Platform”
[2] Engelska: ”Trusted Platform Module”

köpa applikationer och spel från marknaden som inte finns tillgängliga i användarens land eller operatör. Precis som Soft-SE är det tillvägagångssätt för SIM-kort att komma ur ett kontrollerat grepp från operatören och ha mer tillgång som användare. Dock uppstår samma fråga som denna avhandlings riktning, är det mjukvarubaserade lösningen ett säkrare alternativ? Mayes och Markantonakis[45] drog slutsatsen att implementering av Software-SIM kan av kostnads- och tidsbegränsnings skäl, inte vara praktiskt att genomföra oberoende säkerhetsbedömningar och låta SIM-leverantören certifiera sina produkter med deras säkerhetslösningar mot SIM-baserade hot och attacker. Kommer Soft-SE bli en upprepning av säkerhetshistoria och sluta upp med samma öde som emulering av SIM-kort?

7.3 SEEK

En av de största anledningarna till att Soft-SE prisas bland tredje parten är på grund av tillgången till det annars låsta elementet. Ett alternativ sätt att få tillgång till det säkra elementet är med hjälp av Secure Element Evaluation Kit(SEEK). SEEK skapades som öppen källstack för kommunikation med SE (t.ex. SIM-kort, inbäddad). SEEK för Android plattformen kallas för Smartkorts API[1][46]. SmartCard API ger funktionalitet som listar och väljer den SE som stödjer enheten, öppnar en kommunikationskanal till det dedikerade säkerhetselementet och överför ”applikations protokolldataenheter[2]”(APDU). APDU är kommunikationsenheten mellan smartkortsläsaren och smartkortet. SmartCard API kan användas för testning och utveckling av Android applikationer som kommunicerar med SE som finns tillgänglig i fysisk format eller i en emulator.

Ytterligare några API:s som har föreslagits av Michel Roland[35] för tillgång av säkerhetselementer är JSR 177, Nokias Extensions till JSR 257 och BlackBerry 7 API. Vissa av dessa API beviljas åtkomsten endast med pålitlig signatur från tillverkaren eller operatören.

[1] Engelska: ”SmartCard API”
[2] Engelska: ”Application Protocol Data Unit”

8 Slutsats

Denna avhandling har utvärderat ett par säkerhetsrisker på både det säkerhetselement som används i dagsläget och de nya applikationsbaserade elementet. Den har även utvärderat för- och nackdelar med att implementera Soft-SE. I analysen diskuterades några alternativa vägar som en användare kan ta del av för att tillämpa några av de fördelar som Soft-SE har utan att emulera en smarttelefon. Det nuvarande elementet har utsatts för många hot och attacker och med tiden uppkommer det ständigt nya skadliga program. Vare sig någon bestämmer sig för att hålla sig till det säkerhet som redan erbjuds eller det alternativa säkerhetselementet så kommer det alltid finnas hot och attacker som en användare måste vara medveten om. Det går inte skydda sig mot allt men det går att skydda sig från en del säkerhetsattacker och vissa former av säkerhetselement är mindre utsatta än andra. Dock besitter inte alla användare den kunskap som krävs för att skydda sig mot de möjliga attackerna från deras personliga data och kommer därför att hellre lita på den säkerhetslagring som har certifierats av leverantörer och operatörer.

Soft-SE är det alternativet utvecklarna kommer gå efter eftersom det inte finns några mellanhänder och ytterligare parter inblandade. Soft-SE kan användas som ett alternativ för P2P läget för kommunikation mellan två NFC-enheter. Dock råder det signifikanta säkerhetsbrister vid användning av Soft-SE och det blir svårare att skydda innehållet av emulerade kort. Soft-SE drar ingen nytta av säkerhetsdatalagringen och brist på exekveringsmiljö kan leda till avsiktliga störningar av andra applikationer. Dessutom gör den mobilen till en ideal plattform för genomföring av relä attacker på smartkort och andra kortemulerings applikationer. Slutligen begränsas användningen av Soft-SE på enheter av telefontillverkarna samt chipsettillverkare. Däremot kan många applikationer av Soft-SE implementeras i P2P läget men detta kräver signifikanta uppgraderingar av existerande infrastruktur.

Min slutsats utifrån denna avhandling är att Soft-SE inte är ett säkrare val och dessutom inte nödvändig för NFC-enheter, då de flesta applikationer kan använda sig av P2P läget som skapades för enkel kommunikation mellan NFC-enheter. Såvida tekniken inte vidareutvecklas till ett säkrare alternativ, är det bättre att fortsätta använda SE som kommer i formerna UICC, SD och inbäddad. Ägarna av säkerhetselementen borde överväga att ge en tredje part möjligheten att vidareutveckla SE, då Soft-SE inte tillför något nytt för allmänheten. För applikationer som Google Wallet där autentiseringsuppgifter sparas i säkerhetselementet borde användarna hålla sig till det operatörer, leverantörer och tillverkarna förser eftersom Soft-SE är fortfarande i en ny stadie av forskning och utveckling. För att Soft-SE ska räknas som ett alternativ måste den främst testas och vidareutveckla sin säkerhetslagring på applikationer som Google Wallet där känslig information är inblandade. Ifall Soft-SE utvecklas tillräckligt för att förhindra många av attackerna kommer det bli ett populärt alternativ hos många NFC användare och inte bara bland utvecklarna. Det kommer dessutom bli ett enklare val för vissa att använda en emulerad mobiltelefon som funkar som ett ”virtuellt kort” på moderna infrastrukturläsare istället för fysiska kort. För övrigt är inte applikationer som Google Wallet tillräckligt säkra i sig då det räcker med att knappa in en fyrsiffrig kod för att komma åt betalningssystemet. Betalningsapplikationerna måste tillämpa ett säkrare system utöver pinkods identifiering för att tillföra den säkerhet som inte ett element kan ge.

8.1 Framtida projekt

Ett framtida koncept för interna, externa och applikationsbaserad SE ska *Inside Secure* erbjuda molnbaserad SE till kunderna om två till tre år[47]. Detta är ett nytt koncept där känslig data sparas i moln istället för själva mobiltelefonen. Vid en fullföljd transaktion med POS-terminal hämtas data från ett virtuell SE i molnen i krypterad form. Broadcom har ett kommande chip BCM43341 som har lyckats linda in NFC, Bluetooth 4.0, WiFi och FM Radio, allt i ett. Detta chip ska stödja flera säkerhetselement samtidigt[48].

Vidare forskning baserat på denna avhandling är att fysiskt testa samma slags attack som till exempel en form av reläattack på en enhet som använder sig något av form av det nuvarande SE:n och en enhet där Soft-SE har tillämpats. Utifrån attacken kan man mäta sårbarheten på de två enheterna och vilken som snabbast kan återhämta sig efter en sådan attack.

8.2 Obligatoriska reflektioner

I denna avhandling har jag jobbat med att utvärdera risker samt analysera de säkerhetselement som finns och använts i NFC-kompatibla telefoner. Jag bestämde mig att fokusera på säkerheten utifrån betalningsdelen av NFC eftersom det området är viktigast för användarna som inte vill bli utsatta av hot och attacker. Ju mer jag satte mig in i ämnet desto mer intresserad blev jag eftersom det är en teknik som väldigt många kommer att implementera till sitt vardagliga liv och då kommer det vara viktigt att veta sina val på hur man vill säkerhetsställa sin enhet som sparar ens privata information. Dessvärre är det brist på information, tillämpning och analys av Soft-SE vilket gjorde det svårare för mig att förstå det nya konceptet. Däremot finns det rikligt med information och rapporter om SE och dess säkerhet som jag kunde utgå från i min avhandling. Min slutsats är att Soft-SE är i nuläget inte säkrare än det traditionella säkerhetselementet och rekommenderar att användaren ska hålla sig till det säkerhetselement som redan ingår i telefonen eller som erbjuds av leverantörer och operatörer tills utvecklarna av Soft-SE har testat och överkommit de säkerhetsrisker som råder över det nya mjukvarubaserade elementet.

Referenser

[1] "A smart, virtual wallet for in-store and online shopping – Google Wallet," *Google Wallet*. [Online]. Available: http://www.google.com/wallet/. [Accessed: 13-Mar-2013].

[2] J. Helzer, "A Look At Near Field Communications Secure Element Chip Suppliers."

[3] G. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," University of Cambridge, Computer Laboratory JJ Thomson Avenue, Cambridge.

[4] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones," Royal Holloway University of London, Information Security Group, Smart Card Centre.

[5] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," School of Electrical Engineering, Tel Aviv University.

[6] "Near Field Communication (NFC) | | Mobil reklam | mobil marknadsföring | mobil hemsidaMobil reklam | mobil marknadsföring | mobil hemsida." [Online]. Available: http://www.advmedia.se/near-field-communication-nfc. [Accessed: 08-Mar-2013].

[7] "Om NFC-teknik." [Online]. Available: http://docs.blackberry.com/en/smartphone_users/deliverables/42332/1783844.jsp. [Accessed: 08-Mar-2013].

[8] I. Al Tal, "Visa and Network International unveil mobile POS terminals in UAE | Visa International | AMEinfo.com." [Online]. Available: http://www.ameinfo.com/visa-network-international-unveil-mobile-pos-323427. [Accessed: 08-Mar-2013].

[9] M. Lewan, "Google har startat sin mobila plånbok," *NyTeknik*. [Online]. Available: http://www.nyteknik.se/nyheter/it_telekom/mobiltele/article3271386.ece. [Accessed: 08-Mar-2013].

[10] J. Van Camp, "How Google Wallet works | Digital Trends," *Digital Trends*. [Online]. Available: http://www.digitaltrends.com/mobile/how-google-wallet-works/. [Accessed: 08-Mar-2013].

[11] N. Elenkov, "Android Explorations," *Emulating a PKI smart card with CyanogenMod 9.1*. .

[12] C. Abraham, "» Return of NFC: Curse of the Secure Element Drop Labs," *Drop Labs*, 06-Mar-2013. [Online]. Available: http://www.droplabs.co/?p=742#more-742. [Accessed: 12-Apr-2013].

[13] "NFC Card Emulation on android – Google Grupper." [Online]. Available: https://groups.google.com/forum/m/?fromgroups#!topic/android-developers/oJzeLJALdG8. [Accessed: 15-Apr-2013].

[14] "Standard ECMA-340," *ECMA International*. [Online]. Available: http://www.ecma-international.org/publications/standards/Ecma-340.htm. [Accessed: 17-Sep-2012].

[15] "NFC Forum: home." [Online]. Available: http://www.nfc-forum.org/home. [Accessed: 08-Mar-2013].

[16] M. Clark, "Java library implements SNEP • NFC World," *NFC World*. [Online]. Available: http://www.nfcworld.com/2012/06/01/316033/java-library-implements-snep/. [Accessed: 22-Apr-2013].

[17] Vedat Coskun, Kerem Ok, and Busra Ozdenizci, *Professional NFC Application Development for Android*. John Wiley & Sons, 2013.

[18] M. Roland, "Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?," 2012.

[19] "DefCon 2012 - Near-Field Communication / RFID Hacking - Miller." [Online]. Available: http://www.slideshare.net/the_netlocksmith/defcon-2012-nearfield-communicationrfid-hacking-miller. [Accessed: 12-May-2013].

[20] “Type 4 Tag Operation Specification,” *NFC Forum*. [Online]. Available: http://apps4android.org/nfc-specifications/NFCForum-TS-Type-4-Tag_2.0.pdf. [Accessed: 27-Apr-2013].
[21] A. Cruz, “NFC AND MOBILE PAYMENTS TODAY,” UNIVERSIDADE DE LISBOA.
[22] E. Lee, “NFC Hacking: The Easy Way.” [Online]. Available: http://www.blackwinghq.com/assets/labs/presentations/EddieLeeDefcon20.pdf.
[23] C. Mulliner, “Hacking NFC and NDEF: why I go and look at it again.”
[24] P. Holman, How to hack RFID-enabled Credit Cards for $8 (BBtv), 2008.
[25] A. Sebastian, “Black Hat hacker lays waste to Android and Meego using NFC exploits | ExtremeTech,” *ExtremeTech*. [Online]. Available: http://www.extremetech.com/computing/133501-black-hat-hacker-lays-waste-to-android-and-meego-using-nfc-exploits. [Accessed: 14-May-2013].
[26] N. McAllister, “Researchers reveal NFC subway bonk-nonpayment scheme • The Register,” *The Register*. [Online]. Available: http://www.theregister.co.uk/2012/09/24/nfc_transit_ticket_hack/. [Accessed: 14-May-2013].
[27] “Alliance Activities: Publications: NFC Frequently Asked Questions - Smart Card Alliance,” *Smart Card Alliance*. [Online]. Available: http://www.smartcardalliance.org/pages/publications-nfc-frequently-asked-questions#7. [Accessed: 17-Nov-2012].
[28] “Alternatives for Banks to offer Secure Mobile Payments,” *Mobey Forum*. [Online]. Available: https://www.nacha.org/userfiles/File/The_Internet_Council/Resources/MObey%20Forum%203%20-%202010%20-%20Alternatives%20for%20Banks.pdf. [Accessed: 17-Nov-2012].
[29] S. Clark, “RIM releases BlackBerry NFC APIs • NFC World,” *NFC world*. [Online]. Available: http://www.nfcworld.com/2011/05/31/37778/rim-releases-blackberry-nfc-apis/. [Accessed: 21-Nov-2012].
[30] “net.rim.device.api.io.nfc.emulation (BlackBerry JDE 7.0.0 API Reference),” *Blackberry*. [Online]. Available: http://www.blackberry.com/developers/docs/7.0.0api/net/rim/device/api/io/nfc/emulation/package-summary.html. [Accessed: 21-Nov-2012].
[31] “Emulating a PKI smart card with CyanogenMod 9.1.” [Online]. Available: http://nelenkov.blogspot.se/2012/10/emulating-pki-smart-card-with-cm91.html. [Accessed: 08-Mar-2013].
[32] S. Clark, “SimplyTapp proposes secure elements in the cloud • NFC World,” *NFC World*. [Online]. Available: http://www.nfcworld.com/2012/09/19/317966/simplytapp-proposes-secure-elements-in-the-cloud/. [Accessed: 21-Nov-2012].
[33] J. Mäntylä, “Analys och förbättring ar av datasäkerhet inom dator system i bilar,” Åbo Akademi.
[34] M. Roland, “Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack,” University of Applied Sciences Upper Austria, Technical Report.
[35] M. Roland, “Practical Attack Scenarios on Secure Element-enabled”, 2012.
[36] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, “Practical NFC Peer-to-Peer Relay Attack using Mobile Phones,” Information Security Group, Smart Card Centre, Royal Holloway University of London.
[37] E. Haselsteiner and K. Breitfuß, “Security in Near Field Communication (NFC),” Philips Semiconductors.

[38] A. Hoog, “Forensic security analysis of Google Wallet – viaForensics,” *VIAFORENSICCS*. [Online]. Available: https://viaforensics.com/mobile-security/forensics-security-analysis-google-wallet.html. [Accessed: 27-May-2013].
[39] J. Rubin, “Google Wallet Security: PIN Exposure Vulnerability - zveloBLOG,” *zveloBLOG*. [Online]. Available: https://zvelo.com/blog/entry/google-wallet-security-pin-exposure-vulnerability. [Accessed: 27-May-2013].
[40] M. Roland, “Personal Communication,” 07-Jan-2013.
[41] “Publications | Nokia Research Center.” [Online]. Available: http://research.nokia.com/publications. [Accessed: 10-Jun-2013].
[42] M. Rouse, “What is trusted platform module (TPM)? - Definition from WhatIs.com,” *WhatIs.com*. [Online]. Available: http://whatis.techtarget.com/definition/trusted-platform-module-TPM. [Accessed: 10-Jun-2013].
[43] “TrustZone - ARM,” *ARM*. [Online]. Available: http://www.arm.com/products/processors/technologies/trustzone.php. [Accessed: 10-Jun-2013].
[44] “Download MarketAccess 1.0.6 for Android Free - MarketAccess emulates the SIM card of the chosen operator and makes paid apps accessible in the Android Market.,” *SOFTPEDIA*. [Online]. Available: http://handheld.softpedia.com/get/Internet-Utilities/Misc-Shopping/MarketAccess-106299.shtml. [Accessed: 08-May-2013].
[45] K. Mayes and K. Markantonakis, “Mobile Communication Security Controllers,” Royal Holloway, University of London.
[46] “UsingSmartCardAPI - seek-for-android - Writing Android applications with access to Secure Elements using the SmartCard API - Secure Element Evaluation Kit for the Android platform - the ‘SmartCard API’ - Google Project Hosting.”[Online]. Available: http://code.google.com/p/seek-for-android/wiki/UsingSmartCardAPI. [Accessed: 10-Jun-2013].
[47] S. Clark, “Inside Secure to offer cloud-based NFC secure element solution - NFC World,” *NFC World*. [Online]. Available: http://www.nfcworld.com/2012/09/25/318059/inside-secure-to-offer-cloud-based-nfc-secure-element-solution/. [Accessed: 15-Mar-2013].
[48] “Single Chip, Dual-Band (2.4 GHz / 5 GHz) 802.11 g/n MAC/Baseband/Radio with Integrated Bluetooth 4.0, NFC + FM Receiver - BCM43341 | Broadcom,” *BROADCOM*. [Online]. Available: http://www.broadcom.com/products/NFC/NFC-Solutions/BCM43341. [Accessed: 14-May-2013].

TRITA-ICT-EX-2013:136

www.kth.se