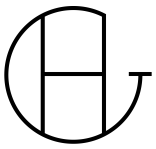


HoGent

Faculteit Bedrijf en Organisatie

Titel

Piet Pieters

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Bert Van Vreckem

Instelling: —

Academiejaar: 2015-2016

Tweede examenperiode

Faculteit Bedrijf en Organisatie

Titel

Piet Pieters

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Bert Van Vreckem

Instelling: —

Academiejaar: 2015-2016

Tweede examenperiode

Woord vooraf

Samenvatting

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus.

Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

1. Inleiding

De inleiding moet de lezer net genoeg informatie verschaffen om het onderwerp te begrijpen en in te zien waarom de onderzoeksvraag de moeite waard is om te onderzoeken. In de inleiding ga je literatuurverwijzingen beperken, zodat de tekst vlot leesbaar blijft. Je kan de inleiding verder onderverdelen in secties als dit de tekst verduidelijkt. Zaken die aan bod kunnen komen in de inleiding (Pollefliet, 2011):

- context, achtergrond
- afbakenen van het onderwerp
- verantwoording van het onderwerp, methodologie
- probleemstelling
- onderzoeksdoelstelling
- onderzoeksvraag
- ...

1.1 Probleemstelling

Uit je probleemstelling moet duidelijk zijn dat je onderzoek een meerwaarde heeft voor een concrete doelgroep. De doelgroep moet goed gedefinieerd en afgelijnd zijn. Doelgroepen als "bedrijven," "KMO's," systeembeheerders, enz. zijn nog te vaag. Als je een lijstje kan maken van de personen/organisaties die een meerwaarde zullen vinden in deze bachelorproef (dit is eigenlijk je steekproefkader), dan is dat een indicatie dat de doelgroep goed gedefinieerd is. Dit kan een enkel bedrijf zijn of zelfs één persoon (je co-promotor/opdrachtgever).

1.2 Onderzoeksvraag

Wees zo concreet mogelijk bij het formuleren van je onderzoeksvraag. Een onderzoeksvraag is trouwens iets waar nog niemand op dit moment een antwoord heeft (voor zover je kan nagaan). Het opzoeken van bestaande informatie (bv. “welke tools bestaan er voor deze toepassing?”) is dus geen onderzoeksvraag. Je kan de onderzoeksvraag verder specifiëren in deelvragen. Bv. als je onderzoek gaat over performantiemetingen, dan

1.3 Onderzoeksdoelstelling

Wat is het beoogde resultaat van je bachelorproef? Wat zijn de criteria voor succes? Beschrijf die zo concreet mogelijk.

1.4 Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

In Hoofdstuk 2 wordt een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein, op basis van een literatuurstudie.

In Hoofdstuk 3 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.

In Hoofdstuk 4, tenslotte, wordt de conclusie gegeven en een antwoord geformuleerd op de onderzoeksvragen. Daarbij wordt ook een aanzet gegeven voor toekomstig onderzoek binnen dit domein.

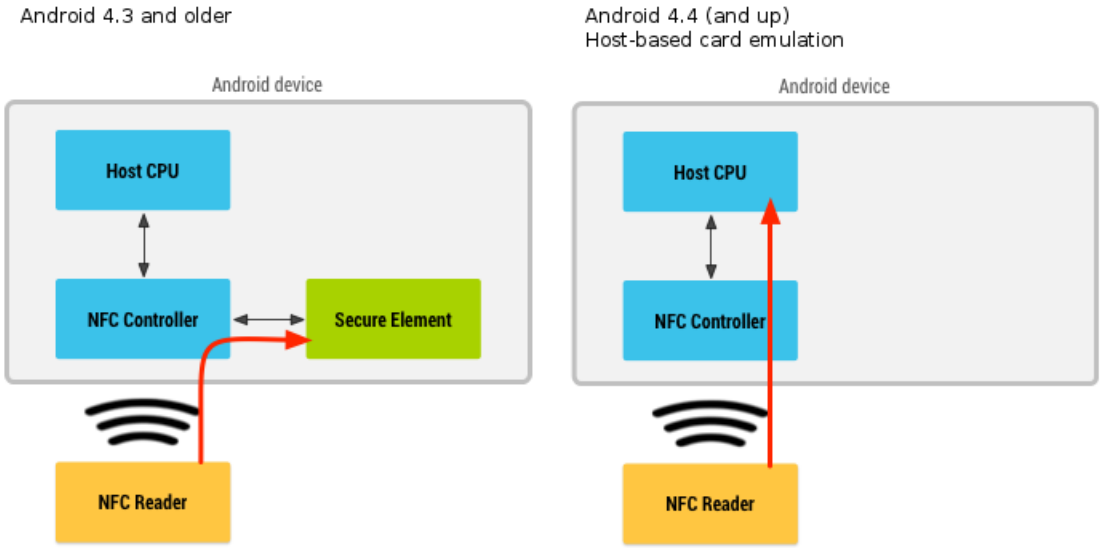
2. Stand van zaken

In dit hoofstuk zal er een stand van zaken gegeven worden van het onderwerp, hoe het vroeger gebeurde en hoe het tegenwoordig gebeurt. Eerst en vooral zal sectie 2.1 wat meer uitleg geven over HCE en hoe het simuleren van draadloze smart cards gebeurt. In sectie 2.2 zal een korte uitleg gegeven worden over NFC technologie. Ten slotte zal in sectie 2.3 uitgelegd worden welke manieren er bestaan om HCE te beveiligen.

2.1 Host-based Card Emulation (HCE)

Sinds de komst van Android 4.4 oftewel Android KitKat introduceerde Google een nieuwe technologie genaamd Host-based Card Emulation (HCE). HCE technologie maakt het mogelijk om Near Field Communication (NFC) technologie te gebruiken zonder de aanwezigheid van een secure element. Wanneer het Android toestel zich in card emulation (CE) mode bevindt en tegen een draadloze leer of point-of-sale (POS) terminal gehouden wordt, heeft het toestel de mogelijkheid om allerhande soorten draadloze smart cards te simuleren. Deze contactloze smart cards worden in vele situaties gebruikt zoals bij draadloos betalen, loyalty systemen, ticketing, toegang tot gebouwen,... (Alliance, 2014).

HCE maakt het dus mogelijk voor NFC apparaten om draadloze smart cards te simuleren. Om gebruik te kunnen maken van HCE heeft android verschillende libraries en APIs (Application Programming Interface) geimplementeerd in het besturingssysteem. Deze libraries en APIs worden overschreven door de applicaties die hier gebruik van willen maken en die op de CPU van het apparaat draaien, deze applicaties kunnen dan APDU (Application Protocol Data Unit) commando's en antwoorden uitwisselen met een NFC POS. Wanneer men vroeger gebruik wou maken van de NFC technologie kon dit alleen



Figuur 2.1: Simulatie van een smart card via SE

door een Secure Element (SE) die ingebouwd zat in het apparaat zoals een SIM kaart. De applicaties werden geïnstalleerd op dit SE die dan de APDU's afhandelde om zo draadloze smart cards veilig te kunnen simuleren. De APDU's die verstuurd worden van een NFC lezer worden opgevangen door de NFC antenne van het appparaat en wordt doorgegeven via de NFC controller naar het SE en omgekeerd zie figuur. Met HCE is het de bedoeling dat de nood van een SE verwijdert wordt uit deze operatie, ipv de APDU's door te geven naar het SE worden deze door gegeven naar de CPU van het apparaat en omgekeerd zie figuur 2.1 (Alattar, 2014).

2.2 Near Field Communication (NFC)

Near Field Communication (NFC) is een technologie die communicatie vanop korte afstanden, meestal nul tot vier centimeter maar kan tot 20 centimeter oplopen, mogelijk maakt. NFC apparaten kunnen actief of passief zijn, wanneer het NFC apparaat actief is dan gebruikt dit apparaat zijn eigen energiebron om zijn radio frequentie te genereren. Een passief NFC apparaat gebruikt de energiebron van een actief NFC apparaat om data te versturen, passieve NFC apparaten kunnen ook enkel maar antwoorden op aanvragen die vanaf een actief NFC apparaat verstuurd wordt. Transacties worden automatisch gestart door twee NFC apparaten elkaar te laten raken of deze twee dicht bij elkaar te houden (Alattar, 2014).

NFC heeft drie verschillende operating modes: Peer to Peer mode, Reader/Writer mode en Contactless Card Emulation. Peer To Peer mode biedt de mogelijkheid om data te versturen tussen twee NFC apparaten aan snelheden tot 424 Kbit/s. Reader/Writer mode maakt het mogelijk dat twee NFC apparaten gebruikt kunnen worden voor het lezen/schrijven van

tags en draadloze smart cards, hierbij is de snelheid van het versturen van de data maar 106 Kbit/s. Contactless Card Emulation laat de NFC apparaten draadloze smart cards of tags simuleren die gelezen of naar geschreven kunnen worden door een NFC lezer (Alattar, 2014).

2.3 Beveiliging HCE

Met de komst van Host-base Card Emulation sinds Android 4.4 is er geen nood meer voor een Secure Element. HCE brengt wel een aantal beveiligingsrisico's met zich mee. Bij een simulatie van smart cards via SE wordt de applicatie geïnstalleerd op het Secure Element, aangezien het Secure Element hardware matig beveiligd is tegen fraude is de applicatie automatisch ook beveiligd tegen veiligheids bedreigingen. Wanneer er gekozen wordt voor een HCE gebaseerde simulatie wordt de applicatie gewoon op het apparaat geïnstalleerd en is deze niet meer beveiligd tegen bedreigingen van andere applicaties die ook op het apparaat staan. Doordat de communicatie tussen de NFC controller en de HCE applicatie niet meer beveiligd is kan de communicatie tussen deze twee onderschept worden door andere malware applicaties. Malware applicaties vormen een groot gevaar voor uw Android toestel, deze malware applicaties kunnen het besturingssysteem aanval. Het risico van een aanval op het besturingssysteem wordt ook vergroot door exploiting, rooting of jailbreaking van het Android toestel. De malware applicatie kan ook de mogelijkheid hebben om exploiting, rooting of jailbreaking zelf te doen of de gebruiker in de val lokken om dit te doen (Alliance, 2014). Om deze bedreigingen tegen te gaan biedt de technologie de dag van vandaag een waaier van mogelijke oplossing die hiervoor ingezet kunnen worden:

- White box cryptography
- Tamper proofed software
- Biometric factors
- Device identity solutions
- Security frameworks/trusted execution environment
- Encryption
- Tokenization
- Bijkomende beveiliging voorzien door een SE

2.3.1 White Box Cryptography

White box cryptography wordt gebruikt om geheimen/sleutels die in het geheugen of in code zitten te verbergen, het is een soort van verduistering die gebruikt wordt voor deterministische algoritmen, dit zijn algoritmen waarbij een bepaalde input altijd dezelfde output terug geeft, en wordt vooral toegepast op cryptografische algortimen. Bij white box implementaties wordt een cipher omgevromd tot een krachtige vorm waar het geheim/sleutel gecombineerd wordt met de code zodat het geheim/sleutel moeilijk afgeleid of herkent kan worden (Alliance, 2014).

2.3.2 Tamper-Proofed Software

Tamper proofing software is een extra beveiligingslaag in de software die ervoor zorgt dat het moeilijker is voor aanvaller om da code statische of dynamische aan te passen of reverse engineering te doen van de code. Dit kan gebeuren op verschillende manieren, runtime integrity checking, breakpoint defenses, obfucation, anti-debug, ... Wanneer er een aanval wordt gedaan en ook effectief word waargenomen door de software zal het tamper-proofed systeem een antwoord produceren waardoor het programma niet goed meer werkt en de aanval wordt verhindert (Alliance, 2014).

2.3.3 Biometric Factors

Biometric factors of biometrische factoren kunnen gebruikt worden bij de authenticatie van een gebruiker in Host-based Card Emulation applicaties. Biometrische factoren worden meestal gebruikt in samenwerking met andere authenticatie middelen. Wat biometrische factoren zo aantrekkelijk maakt bij de authenticatie van gebruiker is voornamelijk de gebruiksvriendelijkheid, zeker in vergelijking met het bijhouden van meerdere wachtwoorden. Er bestaan verschillende soorten biometrische factoren die gebruikt kunnen worden: vingerafdruk, gezichtsherkenning, irisscan en stemherkenning. Deze biometrische factoren zitten al een tijdje geïntegreerd in de meeste laptops en smartphones en kunnen dus gemakkelijk op applicatie niveau gebruikt worden. Een bijkomend probleem is de privacy en beveiliging omtrent de biometrische data die ook in achting genomen zal moeten worden bij het implementeren van de applicatie (Alliance, 2014).

2.3.4 Device Identity Solutions

Device identity solutions gebruiken online diensten voor authenticatie van een toestel die zorgen voor een extra beveiligingslaag voor de Host-based Card Emulation applicaties. Fast Identity Online (FIDO) is een voorbeeld van zo een online dienst. FIDO maakt gebruik van publieke sleutel cryptografie technieken voor online authenticatie, het toestel van de gebruiken creëert een sleutel paar waarbij de privé sleutel bijgehouden wordt en de publieke sleutel geregistreerd wordt bij de online dienst. Het authentificeren van het toestel bij de online service wordt gedaan door middel van de privé sleutel die enkel lokaal ontgrendeld kan worden via biometrische factoren of door het ingeven van een PIN code. FIDO ondersteunt veel verschillende technologieën die naaste elkaar gebruik kunnen worden zoals tokenisatie en one-time-password oplossingen. PayPal was een van de eerste die gebruik heeft gemaakt van vingerafdruk verificatie op de Samsung Galaxy S5 met FIDO Ready software (Alliance, 2014).

2.3.5 Security Frameworks/Trusted Execution Environment

Trusted Execution Environment (TEE) is een veilige plaats in de hoofd processor of coprocessor van het toestel waar data kan opgeslagen en verwerkt worden. De bedoeling van een TEE is het uitvoeren van geautoriseerde beveiligingssoftware in een vertrouwde omgeving.

TEE bestaat niet enkel uit sofware maar ook uit hardware die bescherming bieden tegen aanvallen vanuit het rich operating system (Rich OS) in het toestel. Gevoelige applicatie die beschermt moeten worden van Rich OS worden opgeslagen in de TEE en helpt ook bij de controle van toegangsrechten tot de applicaties. TEE heeft zijn eigen besturingssysteem, hierdoor kan de TEE niet aangetast worden wanneer het besturingssysteem van het toestel aangetast is. De TEE kan voor een extra beveiligingslaag zorgen voor HCE applicaties:

- **PIN/wachtwoord ingave.** De TEE kan extra bescherming aanbieden aan de hand van het invoeren van een PIN code of een wachtwoord, bij de TEE is de invoer van de PIN code of een wachtwoord volledig gescheiden van de invoer van het toestel, hierdoor kan de invoer niet onderschept worden door malware applicaties die zich op het besturingssysteem van het toestel bevinden.
- **Secure storage of credentials.** De TEE implementeerd cryptografische operaties binnen de secure execution environment en zorgt voor het veilig opslaan van sleutels. Hierin kunnen dus tokens/sleutels van betaling applicaties in opgeslagen worden, zo zijn deze beter beveiligd tegen aanvallen dan wanneer ze opgeslagen worden in het besturingssysteem van het toestel.
- **Secure transfer protocol endpoint.** Het is mogelijk om in de TEE een geëncrypteerd beveiligd kanaal op te zetten van de kant van de terminal. Dit betekent dat de APDU's geëncrypteerd verstuurd kunnen worden van de terminal en de HCE applicatie via een draadloze interface naar de TEE. Een tweede geëncrypteerd beveiligd kanaal kan opgezet worden tussen de TEE en een Cloud applicatie. Hierdoor zijn de sleutels en data enkel zichtbaar binnen de vertrouwde applicatie, dit biedt een hoger niveau van beveiliging dan wanneer de applicatie uitgevoerd zou worden op het besturingssysteem van het toestel.

2.3.6 Encryption

2.3.7 Tokenization

2.3.8 Secure Element

3. Methodologie

4. Conclusie

A. Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1 Introductie

Tegenwoordig worden smart-cards zoals bankkaarten, klantenkaarten, ... maar al te vaak vervangen door digitale versies op smartphones en smartwatches. Dit verloopt via NFC of "Near Field Communication". Hiervoor wordt er normaal gezien een secure-element gebruikt die zorgt voor de beveiliging en de communicatie. Sinds Android4.4 (KitKat) is het mogelijk om dit te doen via HCE of "Host-based card emulation". Eén van de nadelen van deze technologie is het veiligheidsrisico die het met zich meebrengt. Android HCE maakt het gemakkelijker om de NFC technologie te gebruiken omdat er geen nood meer is aan een secure-element, waardoor er dus ook geen commerciële overeenkomst meer moet afgesloten worden met de secure-element verdelers. Het doel van deze paper is om na te gaan hoe men Android HCE op een veilige manier kan gebruiken voor allerhande betalingssystemen.

A.2 State-of-the-art

Door het gebruik van Android HCE is er een groot veiligheidsrisico. Dit doordat er geen gebruik meer wordt gemaakt van een secure-element die zorgt dat alle gegevens van de gebruiker veilig worden opgeslagen. Volgens de paper van Smart Card Alliance (Alliance, 2014) zijn de twee meest voorkomende manieren om met Android HCE te

werken via de cloud met een token en zonder token. Zonder token werken wordt niet als veilig aanschouwd doordat betalingsgegevens gemakkelijk ontdekt kunnen worden door malware. Het gebruik maken van een token verlaagt de kans niet tot het ontdekken van betalingsgegevens door malware, maar het verlaagt wel de impact van een eventuele ontdekking door het vervangen van statische betalingsgegevens met een token. Nadelen van het gebruiken van Android HCE (Lepojevic, Pavlovic & Radulovic, 2014) in vergelijking met een normale Smart Card is dat HCE niet werkt zonder stroom. Wanneer er geen verbinding kan gemaakt worden met de cloud kan HCE de authenticatie niet voltooien.

A.3 Methodologie

Om de veiligheid te kunnen testen zal er een proof of concept opgesteld worden met drie verschillende beveiligingsmethodes namelijk Tokenisatie, Encryptie en biometrische factoren. Hierbij kan er dan vergeleken worden hoe veilig ze zijn ten opzichte van elkaar en ten opzichte van het gebruiken van een secure-element. Bij het vergelijken van de verschillende methoden zal er gekeken worden naar welke gegevens leesbaar zijn, hoe gemakkelijk het is om deze methoden te omzeilen, ... Er zal gebruikgemaakt worden van OWASP The Mobile Security Testing Guide om zo de verschillende veiligheidsproblemen op te sporen in de applicatie. Verder wordt ook de moeilijkheidsgraad gemeten van iedere implementatie zodat er een besluit kan gemaakt worden welke oplossing bij welke use case het best gebruikt kan worden.

A.4 Verwachte resultaten

Het resultaat zal bestaan uit verschillende proof of concepts waarbij het gebruik van Android HCE toch op een veilige manier benut kan worden. Op basis van de resultaten zal dan ook beslist kunnen worden welke implementatie het beste is voor welke use case.

A.5 Verwachte conclusies

Verwacht wordt dat de verschillende implementaties tot beveiligde applicaties leiden waarbij NFC technologie gebruikt kan worden via Android HCE. Alsook dat de applicatie met de biometrische factoren het veiligste zal zijn en hierbij de user experience het beste zal zijn omdat dit ook een groter gevoel van veiligheid geeft.

Bibliografie

Alattar, M. (2014). Host-based Card Emulation: development, security, and ecosystem impact analysis.

Alliance, S. C. (2014). A Smart Card Alliance Mobile & NFC Counci White Paper - Host Card Emulation (HCE) 101.

Lepojevic, B., Pavlovic, B. & Radulovic, A. (2014). Implementing NFC Service Security.

Pollefliet, L. (2011). *Schrijven van verslag tot eindwerk: do's en don'ts*. Gent: Academia Press.