Verschillende veiligheidsmethodes voor Android HCE (Host-based Card Emulation)

Onderzoeksvoorstel Bachelorproef

Thibaut Maddelein[1]

Samenvatting
In deze Bachelorproef zal er onderzoek gedaan worden naar hoe je Android Host-based Card Emulation (HCE) op een veilige manier kan gebruiken. Aangezien er tegenwoordig allerlei smart-cards zoals bankkaarten, klantenkaarten, ... gedigitaliseerd worden zijn er vele use cases voor het gebruik van NFC techonologie. Vroeger kon dit enkel via een secure-element maar sinds Android4.4 (KitKat) kan men gebruik maken van Android HCE. Deze techniek brengt veel veiligheidsrisico's met zich mee zoals ongeëncrypteerde betalingsgegevens. Er zijn een aantal beveiligingsmaatregelen die geimplementeerd kunnen worden in de applicatie zodat het gebruik van Android HCE toch op een veilige manier kan gebruiken. Er zullen een aantal proof of concepts gemaakt worden met verschillende beveiligingsmaatregelen. De verschillende implementaties worden vergeleken op vlak van veiligheid en moeilijkheidsgraad om te implementeren. Hierbij wordt er verwacht dat de verschillende implementaties tot een veilige applicatie leiden. Verder lijkt de implementatie met biometrische factoren zoals vingerscan één van de veiligste oplossingen zal zijn en ook de meest gebruiksvriendelijke, omdat dit ten eerste zelf waargenomen kan worden door de gebruiker. Ten tweede geeft het een groter gevoel van veiligheid. Op dit moment zijn er al vele use cases waarin deze implementaties al gebruikt kunnen worden en er zullen er nog vele bijkomen in de toekomst.

Sleutelwoorden
Mobiele applicatieontwikkeling. Android — Host-based Card Emulation — NFC

Co-promotor
Francesco Verheye[2] (CCV Lab)

Contact: [1] thibaut.maddelein.y9677@student.hogent.be; [2] f.verheye@ccvlab.eu;

Inhoudsopgave

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.

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.

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.

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.

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.

Referenties

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.