# Wat zijn bekende kwetsbaarheden voor OV-chipkaarten?

OV-chipkaarten zijn speciale kaarten die het reizen in het openbaar vervoer eenvoudiger maken. Door de invoer van OV-chipkaarten is het niet nodig om iedere keer dat je de bus in stapt een kaartje te kopen bij de buschauffeur. Gewoon de kaart tegen de lezer aanhouden wanneer je instapt, en de kaart nog een keer tegen de lezer aanhouden wanneer je uitstapt. Dit principe is mogelijk met behulp van NFC. Dit onderzoek bestaat uit de volgende onderdelen:

Inhoudsopgave

[Wat zijn bekende kwetsbaarheden voor OV-chipkaarten? 1](#_Toc119931366)

[Wat is NFC? 1](#_Toc119931367)

[Wat is RFID? 1](#_Toc119931368)

[Waarvoor wordt NFC nog meer gebruikt? 3](#_Toc119931369)

[Hoe zit een OV-chipkaart in elkaar? 3](#_Toc119931370)

[Zijn er bekende kwetsbaarheden voor NFC? 4](#_Toc119931371)

[Welke onderzoeksmethodes zijn toegepast tijdens dit onderzoek? 4](#_Toc119931372)

[Conclusie 5](#_Toc119931373)

## Wat is NFC?

Near-Field Communication, oftewel NFC is een methode waarmee op korte afstand contactloos gecommuniceerd kan worden. NFC werkt op basis van RFID, dus om te begrijpen wat NFC is, en hoe het werkt, is het belangrijk om te weten wat RFID is. Daarover is hieronder meer info te vinden.

## Wat is RFID?

NFC is een vorm van RFID. RFID staat voor Radio-Frequency Identification. Bij deze technologie wordt data opgeslagen op een minuscule chip, oftewel een RFID-tag. Via radiogolven worden de gegevens van deze chip uitgelezen. De twee meest gebruikte types RFID zijn:

* Passieve RFID. Een passieve RFID-tag heeft geen eigen energiebron, maar maakt gebruik van het elektromagnetische veld van de lezer voor zijn energie. De tag zet deze energie om in een radiofrequentie-golf in de richting van de lezer. De lezer interpreteert deze golven en zet ze om naar data. De meeste passieve RFID-tags hebben enkel een integrated circuit(IC) en een interne antenne. De frequentie van passieve RFID-tags varieert van 125KHz tot 960MHz, waarbij een hogere frequentie leidt tot een groter bereik. De grootste voordelen van passieve RFID-tags zijn het kleine formaat, relatief lage kosten en de lange levensduur(afhankelijk van wear and tear). Ook is er een enorm aanbod van verschillende varianten van passieve tags. NFC maakt gebruik van passieve RFID.
* Actieve RFID. De meeste actieve RFID-tags gebruiken een frequentie van 433MHz of 2,45GHz. Actieve RFID systemen hebben vaak drie onderdelen: een lezer, antenne en een tag. Daarnaast hebben actieve systemen ook een interne batterij, waardoor de “read range”, oftewel vanaf welke afstand het signaal nog te lezen is, heel groot kan zijn, en ze veel geheugen hebben. Deze batterij gaat tussen de drie en vijf jaar mee. Wanneer deze batterij echter faalt, moet de actieve tag vervangen worden. Er zijn twee verschillende types actieve RFID-tags: transponders en beacons. Bij een transponder wordt eerst, net zoals bij passieve RFID, een signaal verstuurd door de lezer, waarna de transponder reactie geeft. Een beacon wacht niet af tot er een signaal binnenkomt, maar stuurt iedere 3-5 seconden specifieke data. De grootste voordelen van actieve RFID-tags zijn de grote “read range” en de mogelijkheden om de tags te koppelen aan andere technologieën, zoals GPS of sensoren.

## Waarvoor wordt NFC nog meer gebruikt?

In het dagelijks leven wordt NFC regelmatig toegepast. Zo maken OV-chipkaarten dus gebruik van NFC-chips om gebruikers in te laten checken in het openbaar vervoer. Een gebruiker houdt de kaart tegen een lezer aan, en wordt automatisch ingecheckt. Om weer uit te checken, houdt de gebruiker de kaart nogmaals tegen de lezer aan. Ook bankpassen maken gebruik van bankpassen om contactloos betalen mogelijk te maken. Naast bankpassen en OV-chipkaarten zijn er nog veel meer passen uitgerust met NFC. Denk bijvoorbeeld aan een medewerkerspas, of een visitekaart.

Ook is nagenoeg iedere smartphone uitgerust met een NFC-chip. Met deze chip is het opzetten van verbindingen met andere apparaten relatief eenvoudig. Zo is het bijvoorbeeld mogelijk om verbinding te maken met bepaalde draadloze speakers via NFC. Ook is het mogelijk om via een NFC tag Wifi in te schakelen, of te verbinden met een wifi netwerk.

## Hoe zit een OV-chipkaart in elkaar?

In OV-chipkaarten zit dus een NFC chip. Toen de OV-chipkaart werd ingevoerd, werd de MIFARE classic gebruikt als chip. Later is gebleken dat deze chip fraudegevoelig was, waardoor de overstap naar een nieuwe chip is doorgevoerd. Deze nieuwe chip, de Infineon SLE-66, wordt nog steeds gebruikt. De hele OV-chipkaart is passief, afgezien van de beveiligingsmodule. Deze controleert door een uitwisseling van codes of de leesapparatuur legitiem is. Verder is op de geheugenkaart van een OV-chipkaart de volgende data te vinden:

* Identificatiegegevens van de kaart: een 14-cijferig kaartnummer, geldigheidsperiode en uitgevend bedrijf. Verder staat op persoonlijke kaarten ook de geboortedatum van de eigenaar.
* Het saldo op de kaart.
* De laatste tien reistransacties. Hierbij geldt inchecken als één transactie, en uitchecken als een tweede transactie. Ook een controle wordt als een transactie geregistreerd. Daarnaast telt ook gebruik van een toeslagzuil als een transactie. De verzameling van de laatste tien transacties wordt dus op de kaart opgeslagen.
* De laatste twee oplaadtransacties. Indien automatisch opwaarderen aan staat, wordt dit ook meegenomen als oplaadtransactie.
* Het gegeven “automatisch opladen” bedrag. Wanneer het saldo van de kaart op is, wordt dit bedrag automatisch opgewaardeerd met een vooraf bepaald bedrag, indien dit geactiveerd is.

De gegevens op de kaart zijn up-to-date. De gegevens worden in de centrale database vertraagd bijgewerkt(duurt vaak één tot anderhalve dag). Hierdoor hebben mensen de mogelijkheid om alsnog uit te checken als ze dit vergeten zijn op het moment dat ze het OV verlaten.

## Zijn er bekende kwetsbaarheden voor NFC?

NFC is natuurlijk niet perfect, en dus zijn er kwetsbaarheden te vinden in NFC-systemen. Zo is op 11-05-2021 een kwetsbaarheid([CVE-2021-32089](https://www.cvedetails.com/cve/CVE-2021-32089/)) gemeld waarbij een aanvaller willekeurige bestanden kan uploaden naar een RFID-tag. Wanneer de tag vervolgens aangeroepen wordt, zullen deze bestanden ook opgestuurd worden naar de lezer. Hierbij bestaat natuurlijk de kans op Cross-Site Scripting. Deze kwetsbaarheid geldt echter alleen op producten die niet meer ondersteund worden door de ontwikkelaar, en geldt dus enkel voor verouderde systemen.

Op 10-03-2021 is een kwetsbaarheid([CVE-2021-0462](https://www.cvedetails.com/cve/CVE-2021-0462/)) gemeld voor NXP NFC firmware. Bij een firmware update voor Android is er een kwetsbaarheid ontstaan. Hierbij is er een relatief klein risico op “escalation of privilege,” oftewel de mogelijkheid om toegang te krijgen tot bestanden waar een gebruiker geen toegang tot hoort te krijgen. Er is geen User Interaction nodig om misbruik te kunnen maken van deze kwetsbaarheid. Ondertussen is ook deze kwetsbaarheid opgelost door middel van een nieuwe update.

Op 10-03-2019 werd een kwetsbaarheid([CVE-2017-15361](https://www.cvedetails.com/cve/CVE-2017-15361/)) werd een kwetsbaarheid gemeld voor de Infineon RSA library. Dit is de enige kwetsbaarheid die van toepassing is op de Infineon SLE-66 die in de OV-chipkaart zit, aangezien deze gebruik maken van de RSA library. RSA-key generation wordt verkeerd afgehandeld, waardoor hackers makkelijker misbruik kunnen maken van cyptografische veiligheidsmerchanismen. Deze kwetsbaarheid is redelijk lastig uit te buiten, en levert niet heel veel schade op.

## Is het mogelijk om een OV-chipkaart te kopiëren?

Simpel gezegd, nee, het is niet mogelijk. De pogingen om een OV-chipkaart uit te lezen, met behulp van een [RFID-reader](https://www.amazon.nl/Frequency-Duplicator-13-56MHz-Encrypted-Keychains/dp/B08DNR1YBB), met de bijbehorende *smart card tool software v2020 wildfire edition Build:210302 software*, zijn lastig samen te vatten, aangezien de resultaten onduidelijk waren. Enerzijds gaven de lezer en de software beide aan dat het kopiëren van de data op de OV-chipkaart succesvol was, maar wanneer ik de data naar een andere pas schreef, werd deze niet geaccepteerd. Dit komt doordat er in de OV-chipkaart een veiligheidscontrole uitgevoerd wordt, en als de status hiervan niet doorgegeven wordt, negeert de lezer de data van de NFC-chip. Dus om een OV-chipkaart te kopiëren, zal eerst de beveiligingscheck nagebootst moeten worden, wat binnen de geschreven uren niet haalbaar is.

## Welke onderzoeksmethodes zijn toegepast tijdens dit onderzoek?

Dit onderzoek is uitgevoerd op basis van het dot framework. Hieronder staat beschreven welke methodes van het dot framework toegepast zijn:

* Library research. Voor dit onderzoek is library research toegepast om erachter te komen of er al andere onderzoeken naar dit onderwerp gedaan zijn. Ook is library research toegepast om erachter te komen of er tools bestaan die het onderzoek kunnen ondersteunen.
* Problem analysis(Field). Om tot een duidelijke hoofdvraag te komen, is een probleemanalyse uitgevoerd voor dit onderzoek.
* Security test(Showroom). Om de veiligheid van een OV-chipkaart in kaart te brengen, is security testing toegepast.

## Conclusie

De hoofdvraag van dit onderzoek luidt als volgt: Wat zijn bekende kwetsbaarheden voor OV-chipkaarten? Deze vraag heeft een relatief eenvoudig antwoord, namelijk dat er nagenoeg geen kwetsbaarheden bekend zijn voor de Infineon SLE-66 chip die in de OV-chipkaart zit. Het kopiëren van de kaarten is, met de juiste kennis en middelen mogelijk, echter is dit niet een gigantisch risico. Wanneer een OV-chipkaart in verkeerde handen valt, spreken we al van een probleem, dus of de kaart nog gekopiëerd kan worden, is niet van grote invloed.