Veilig contactloos betalen

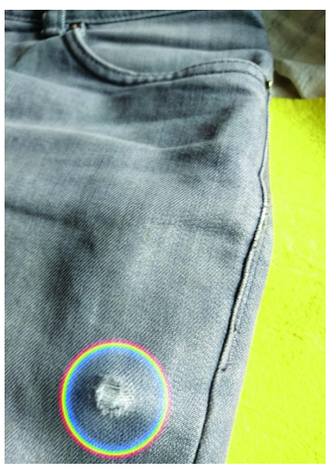
Rinus Alberti

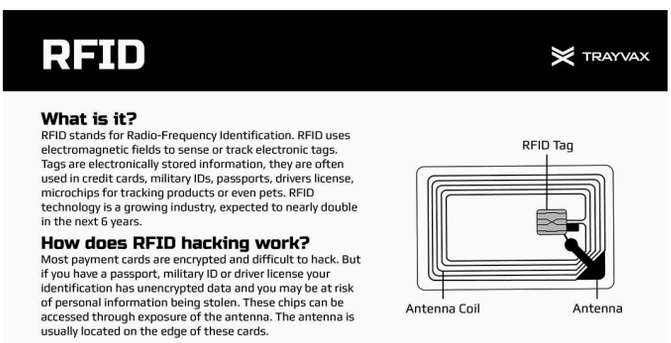
Iemand loopt 'per ongeluk' tegen je aan, mompelt een excuus en loopt weer door. Een niet onalledaagse gebeurtenis in een drukke winkelstraat. Een uur later is je bankrekening geplunderd ...

Dit is het doemscenario dat beveiligingsexperts ons graag voorhouden, evenals aanbieders van beschermende pinpashouders, ook wel 'RFID-protected wallets' genoemd. Hierin wordt je contactloze pinpas volledig beschermd tegen boze invloeden van buiten.
Ook ik heb me hierdoor laten beïnvloeden en een dergelijke pasjeshouder aangeschaft.

Deze pasjeshouder heeft één (twijfelachtig) voordeel. Zoals je ziet kun je een paar kaarten buiten het beschermde gebied opslaan. Bijvoorbeeld je OV-chipkaart, zodat die gemakkelijk te gebruiken is als je op het station staat en je niet verder hoeft te zoeken naar die kaart.
Een bijzonderheid is hier wel dat die kaart nu deels buiten het beschermde gebied valt, maar toch nog voldoende beschermd wordt door het aanwezige metaal.

Deze had slechts één probleem – hij was van metaal en er zaten (door de vereisten bij het ontwerp) scherpe hoeken aan die op den duur ongewenste slijtageplekken aan mijn broeken veroorzaakten. Daar was mijn echtgenote natuurlijk niet gelukkig mee en dat was de reden dat ik via internet op zoek ging naar een andere oplossing.
En dat leverde toch wel enkele verrassingen op die ik jullie hier niet wil onthouden ...
Allereerst wil ik iets kwijt over de term waarmee alles samenhangt: RFID. RFID staat voor Radio Frequency Identification en is een veel toegepaste technologie met zijn roots in het herkennen en transporteren van 'spullen', en dat gaat véél verder dan de toepassing in pinpassen.
Een mooie uitleg hierover (in het Engels) vind je hier:





De essentie van dit verhaal is dat een 'pinpaslezer' een electromagnetisch (radio-)signaal uitzendt en zodra de pinpas binnen het electromagnetische veld van deze paslezer komt, op gecontroleerde wijze, draadloos informatie gaat uitwisselen. Wil je nu al meer weten over RFID en hoe het werkt, kijk dan ook eens op: **https://nl.wikipedia.org/wiki/Radiofrequency_identification**.

In het plaatje zie je ook hoe zo'n kaart er inwendig uitziet en in korte lijnen hoe het hacken (illegaal aftappen van informatie) van een van RFID voorziene kaart werkt.
Want daarover, én hoe je misbruik kunt voorkomen, gaat het verder in dit verhaal.

Meer over RFID-tags

RFID-tags vinden een uitgebreide toepassing op allerlei terreinen. Waren zij in eerste instantie bedoeld om in een productieproces producten te identificeren en logistiek te volgen, tegenwoordig worden ze ook ingezet voor toegangscontrole in ziekenhuizen (vervanging van het bekende armbandje), bij sportwedstrijden, diefstalpreventie, en voor het volgen van dieren – zowel huisdieren alsook wilde dieren in de vrije natuur – om er maar een paar te noemen. Ik heb gehoord dat er zelfs mensen zijn die een RFID-tag onder hun huid laten implanteren om de drankjes in hun stamcafé bij te houden en af te rekenen – bijzonder handig als je van plan bent om daar ladderzat te worden.

Om dit allemaal naar behoren te kunnen doen zijn er verschillende soorten tags op de markt, afhankelijk van het gebruik ervan. Een belangrijk onderscheid wordt gemaakt voor de maximale afstand waarop een tag nog uit te lezen is. Er zijn in dat kader twee soorten tags te onderscheiden: zgn. passieve en actieve tags.

Voor de meest gebruikelijke passieve tags is dat:
- voor korte afstanden - tot 10 cm - worden voornamelijk tags in de LF-band van 125 of 134 kHz gebruikt.
- voor middellange afstanden – tot 1 meter – gebruikt men tags in de HF-band: 13,56 MHz.
- voor nog grotere afstanden wordt de UHF-band gebruikt in de frequentieband van 860 – 960 MHz. Deze afstanden kunnen variëren van 10 tot 15 meter.

Naast passieve tags wordt ook gebruik gemaakt van actieve tags waarin een voedingsbatterijtje verwerkt is. Deze zijn over grotere afstanden – tot honderden meters – te gebruiken. Actieve tags worden niet in contactloze pin-kaarten gebruikt, dus blijven ze hier ook buiten beschouwing.

'Onze' contactloze pin-kaarten opereren in de frequentieband van 13,56 MHz en kunnen op een afstand van ongeveer 2,5 tot 10 cm betrouwbaar uitgelezen worden. De voeding voor hun componenten creëren de passieve tags uit het uit-

gezonden signaalvermogen van de reader in het werkingsgebied waarvan zij zich bevinden. De informatie op de pinkaart is weliswaar encrypted opgeslagen, maar een betaalautomaat kan die probleemloos opvragen ...

Een mooi voorbeeld van het gebruik in sportwedstrijden zijn de (gepersonificeerde) tags die in de sportschoenen verwerkt zijn en die op bepaalde punten in het hardloopparcours worden uitgelezen. Daardoor is het verloop van de wedstrijd eenvoudig en nauwkeurig te volgen.
Ook is onze poes 'gechipt' met een tag onder zijn huid, met informatie over zijn 'huisadres', zodat zijn baasje terug te vinden is wanneer hij wegloopt, of erger. Zijn medische gegevens zijn daarin ook opgeslagen; de dierenarts kan die eenvoudig raadplegen met zijn reader.

Andere voorbeelden van het nut van tags heb ik gezien bij de plaatselijke Kruidvat-vestiging, waar de producten van een tag zijn voorzien. Die wordt bij de kassa verwijderd of uitgezet. De poortjes aan de in/uitgang detecteren dan of alles netjes is afgerekend. Mooi voorbeeld van diefstalpreventie.

RFID – hoe het werkt in een pinpas.

Normaal steek je je pinpas in de gleuf van een pinautomaat, klop je je pincode in, druk je op OK en de betaling wordt gedaan. Een microprocessor in de kaart regelt dit via het contactvlak met de processor in de pinautomaat.

Bij contactloos betalen gaat het een beetje anders. Het te betalen bedrag staat zoals gewoonlijk in het scherm van de pinautomaat, zodat je dat kunt controleren.

De betaalautomaat heeft een vlak aan de zij- of bovenkant waar je vervolgens je pinpas tegenaan moet houden. De betaalautomaat zendt een radiosignaal uit dat door de antenne van je pinpas (zie bovenstaand plaatje) wordt ontvangen.

De pinpas zendt daarop als antwoord een signaal terug waarin o.a. bankrekening en goedkeuring van het gevraagde bedrag staan.
De betaalautomaat verwerkt deze informatie en de rest gaat hetzelfde alsof je op OK gedrukt zou hebben. In Nederland kun je op deze wijze bedragen tot € 25,- betalen zonder je pincode in te voeren, maar met een maximum van € 50,-- per dag. Kom je op een dag boven de € 50,- uit, dan moet je toch je pincode ingeven, al is het bedrag kleiner dan € 25,-Je risico is daardoor max. € 50,ook al is het te betalen bedrag kleiner dan € 25,-. Vergelijkbaar met het risico bij het stelen van je portemonnee. Daarbij is het risico groter omdat je dan ook vaak andere pasjes, zoals je rijbewijs, weer moet aanvragen. Dan ben je nog veel meer geld kwijt. Zie ook: **https://www.pin.nl/consument/contactloos-betalen-met-betaalpas-of-mobiele-telefoon/**
O ja, in het geval van verlies of diefstal vergoedt je bank het afgeschreven bedrag. Dat doen ze niet in het geval van baar geld: **https://www.pin.nl/consument/veiligheid/**

En hoe je je tegen hacken kunt beschermen

Tot zover ging het over de normale gang van zaken in een winkel. Nu over de man (of vrouw) die 'per ongeluk' tegen je aanloopt. Die heeft een soort miniatuur contactloze betaalautomaat onder zijn jas of in een tas verstopt en zorgt dat die in de buurt van de broekzak komt waar je pinpas in zit. Hij heeft er al een bedrag op 'voorgeprogrammeerd', en je pinpas

geeft in no time braaf toestemming om het bedrag van je rekening af te schrijven. Dit gaat probleemloos zolang het bedrag onder € 25,- blijft. Ook voor bedragen boven € 25,- zijn er mogelijkheden (tot duizenden euro's aan toe) om die van je rekening te bemachtigen, maar dat is ingewikkelder en vereist toch nog je pincode. Omdat de werkwijze niet verschilt, ga ik daar niet verder op in. Overigens is dit door de complexiteit van het geheel nauwelijks toepasbaar.
Een informatieve video kun je hier vinden:
https://www.youtube.com/watch?v=J-UlwW9gPuU

De genoemde miniatuurautomaten zijn voor een relatief gering bedrag overal te koop.
Tot zover hoe men te werk gaat om je op deze manier te bestelen.
Hoewel er weinig concrete bewijzen voorhanden zijn van deze manier van werken, zul je – gezien het gemak waarmee dit kan worden gerealiseerd – je er toch tegen willen beschermen.

Ik ga je vertellen hoe!

Het principe is simpel: zorg dat er geen communicatie tussen pinpas en het malafide apparaat tot stand kan komen.
De meest voor de hand liggende manier is die ik tot nog toe heb gehanteerd: afschermen met een metalen omhulsel (zie plaatje aan het begin van dit verhaal) – daar dringen radiogolven niet doorheen. Maar het heeft mij bijna een paar goedzittende broeken gekost en een 'pissige' echtgenote.
Een andere, goedkopere en minder destructieve methode, die ik ook overwogen heb: stop een stuk aluminiumfolie in je broekzak; dat doet ongeveer hetzelfde als het metalen omhulsel in je pasjeshouder. Je kunt dat eventueel meer stevigheid geven door de folie te lamineren.

Voor of achter de pinpas geplaatst maakt niet uit. Het verstoort de communicatie met de pinpas voldoende.
Ook worden er zgn. jammers (speciale kaarten die je bij je andere kaarten in de pashouder stopt) verkocht. Zodra die een signaal van de pinautomaat detecteren wekken ze uit zichzelf een sterk stoorsignaal op waardoor de communicatie tussen het apparaat en pinpas onoverkomelijk verstoord wordt. Daarnaast geven ze met een hoge pieptoon aan dat iemand een poging doet je te rollen.

En dan nu de meest eenvoudige en niets kostende oplossing!

Stop minstens twee pasjes bij elkaar die geschikt zijn voor contactloze communicatie (die dus een RFID-chip hebben). Dat kunnen pinpassen of creditcards van verschillende banken zijn (mits voorzien van het RFID-logo), maar de OV-chipkaart bijvoorbeeld is er ook zo een, en wie heeft die niet? Ook heb ik ergens gelezen dat de nieuwe rijbewijzen met het creditcardformaat de communicatie ernstig kunnen verstoren.

Wanneer deze bij elkaar zittende kaarten aangestuurd worden, gaan ze beide tegelijk antwoorden, wat ontaardt in een Babylonische spraakverwarring die door de kaartlezer niet te ontcijferen is!
Zoek er, als dat nodig is, een leuke en jou bevallende pashouder bij – zonder al die beschreven poespas – en jij bent helemaal gelukkig!

Ten slotte

Nieuwe ontwikkelingen maken het vandaag de dag ook mogelijk om via je smartphone betalingen te verrichten als ware het een (contactloze) pinpas. Dit kan nu nog niet met alle smartphones en bij alle banken, maar dat zal snel veranderen. Je houdt de smartphone bij of tegen de betaalautomaat en de betaling wordt uitgevoerd, als ware het een contactloze pinpas.

Hierbij wordt veelal voor RFID de term NFC gebruikt: NFC staat voor Near-Field Communication en geeft telefoons, tablets en laptops de mogelijkheid data te delen met andere apparaten die NFC hebben. De technologie is een evolutie van de radio-frequency identification (RFID) technologie.

NFC lijkt erg op RFID, maar is gebaseerd op een andere standaard en met opzet gelimiteerd tot communicatie binnen ongeveer 10 cm. Dat is waarom je je telefoon zo dicht bij de contactloze lezer moet plaatsen. Om je telefoon te kunnen gebruiken, moet die aanstaan en eventueel uit de slaapstand gehaald worden. Daarna gaat alles vanzelf.

Ook worden steeds meer contactloze pinpassen nu met NFC uitgerust. Een van de ‘voordelen’ hiervan is dat, wanneer meer kaarten binnen het bereik van een reader aanwezig zijn, ze nu één voor één kunnen worden uitgelezen. De reader moet daarvoor ook met NFC kunnen werken. Gelukkig is dat nog niet zover met de in dit verhaal genoemde miniatuurreaders, maar het kan zeker komen. En dan staat dit verhaal helaas voor een groot deel op losse schroeven ...

Conclusie

Het is dus met simpele en weinig kostende middelen mogelijk om je te beschermen tegen dit soort praktijken – ongeacht of die wel of niet op grote schaal plaatsvinden.
Het doet niets af aan het inmiddels ingeburgerde gebruik en gemak van contactloos betalen.
En wat houdt je tegen om de beschreven risico's op afdoende en eenvoudige wijze – zoals hier geschetst – ongedaan te maken?

Ook kun je overwegen om voortaan je contactloze betalingen niet met je pinpas te doen, maar uitsluitend met je smartphone, als die tenminste die mogelijkheid heeft.
Is dat het geval, dan moet contactloos betalen op je pinpas sowieso aan staan, maar dat was toch al het geval. Zo niet dan moet je dat even aanpassen via je bankapplicatie.

Nog een waarschuwing tot slot!

Veel mensen bewaren – heel roekeloos – al hun pasjes in het hoesje van de Smartphone. In de eerste plaats: dat werkt niet! De contactloze pasjes laten zich ook hier de mond niet snoeren, en overstemmen de smartphone in zijn communicatie...

En hoe verstandig is het wel om al je belangrijke documenten (rijbewijs, kentekenbewijs, OV-kaart, pinpassen, creditcards, verzekeringsbewijzen, ANWB-kaart en wat al niet meer) hier te bewaren?
Bij verlies of diefstal geldt dan: telefoon weg, alles weg! Hoe dom kun je zijn! Dus houd ze apart en berg ze veilig op!

En de dief zelf dan?

Om op deze manier te werk te kunnen gaan moet een crimineel/dief een aantal zaken vooraf regelen, zoals:

- verplichte inschrijving bij de Kamer van Koophandel
- zakelijke bankrekening bij een bank openen
- registratie van de pinautomaat

(nogal omslachtig dus...)

Katvangers en identiteitsfraude

Criminelen zouden heel gemakkelijk op te sporen moeten zijn, via de registratie van het pinapparaat of de gekoppelde bankrekening.
Als de crimineel alles op zijn eigen naam heeft aangevraagd lukt dat natuurlijk wel.

Echter, om dit te voorkomen worden vaak zgn. 'katvangers' ingezet, mensen die hun pinpas tegen betaling even 'uitlenen', en de buit nog voor de rekening kan worden geblokkeerd uit een geldautomaat halen.
Ook voor een KvK-inschrijving zal een beetje crimineel evenmin terugdeinzen: door middel van identiteitsfraude kunnen ze ook daarvoor iemand anders laten opdraaien.

Vergeet niet dat het meestal om kleine bedragen zal gaan (max. € 25 per ‘diefstal’), terwijl daarvoor veel risico genomen moet worden. Vandaar dat deze manier tot nog toe weinig waargenomen is, maar dat kan veranderen ...