



Wijnand Veeneman, universitair docent
e-mail w.w.veeneman@tbm.tudelft.nl

Somberen over de OV-chipkaart

Nova belde. Of ik iets wilde zeggen over de OV-chipkaart.

Want de chipkaart was nieuws, vanwege de gekraakte encryptie. Ik legde uit dat ik geen expert was op het gebied van encryptie, maar dat ik wel kon uitleggen waarom de chipkaart belangrijk was en wat er sowieso mis gaat met de chipkaart.

Ik deed mijn verhaal, de man van Nova luisterde en zei dat ik het goed uit kon leggen. Of ik toch naar de studio wilde komen. Ik benadrukte nog eens dat ik geen expert was op het gebied van encryptie. Maar dat was geen probleem, zei hij.

Encryptie is niet het probleem van de chipkaart. Ik zal u uitleggen waarom. Allereerst, waar komt de huidige aanval op de chipkaart vandaan? Ik weet niet of u het al gezien heeft, het filmpje waarop twee promovendi aan een Amerikaanse universiteit uitleggen wat ze gedaan hadden. Ze etsten laag voor laag een stukje weg van de minuscule MIFARE-chip (de classic) uit de OV-chipkaart (en uit de Oysterkaart van London en nog veel meer kaarten). En ze maakten van elk laagje een foto door een microscoop. Lieten op die foto's beeldherkenningsoftware los die hen hielp bij het uitvogelen hoe de chip in elkaar stak. Ze ontdekten dat de encryptie beter had gekund.

De aanval werd in Nederland overgenomen door een aantal 'onafhankelijke' beveiligingsexperts: onderzoekers op het gebied van open standaarden

voor encryptie. Zij claimden dat de beveiliging 'open' had moeten zijn, dat was altijd beter. Zoals gezegd, ik ben geen expert op het gebied van encryptie. Waar ik wel het een en ander van afweet is hoe wetenschap werkt. In wetenschap worden mensen opgeslokt door de oplossing waar ze onderzoek aan doen. Ik hoor zelden iemand die kernenergie onderzoekt zeggen dat het geen oplossing is voor het CO₂-probleem, of iemand die aan genterapie werkt dat het niet uiteindelijk een medicijn tegen kanker kan opleveren. Maar altijd blijkt de praktijk weerbarstig, want de oplossing moet zo veel meer kunnen dan dat ene. De chipkaart moet niet alleen veilig zijn, maar ook goedkoop en makkelijk in gebruik en nog veel meer.

Ten tweede, de chipkaart vervangt een strook papier met een maximale waarde van 20,40 euro met een glimstrip: de strippenkaart. De glimstrip is de oude beveiliging. De nieuwe beveiliging is de chip met encryptie. Laten we het nieuws eens vanuit dat perspectief bekijken. Als twee promovendi op een conferentie melden dat ze zo'n glimstrip in grote hoeveelheden kunnen maken, dan is dat geen groot nieuws. Terwijl we die dan ook allemaal op een kleurenkopie van de strippenkaart kunnen plakken en daarmee 20 euro verdienen. Encryptie is dus beter dan eerst en dus niet het probleem.

Ten derde, een doel van de chipkaart was minder zwartrijden en dat lukt door de kraak minder goed dan eerst gedacht. Daarbij lijkt zwartrijden nu deels te kunnen op kosten van andere gebruikers. Maar de vervoerders hebben duidelijke

prikkels om daar wat aan te doen en hoe die prikkels werken laat een ander betaalmiddel zien.

U heeft waarschijnlijk in uw portemonnee een kaartje zitten met 16 cijfers op de voorkant en nog drie extra op de achterkant. Dat heet een creditkaart. Die kaart heeft geen chip en u geeft hem vast regelmatig af in een restaurant of u typt de cijfers in op een internetsite. Jaarlijks wordt er wereldwijd voor miljarden gefraudeerd met creditcardgegevens. Er is weinig ophef over, hoewel het kraken veel eenvoudiger is en de winsten veel groter dan voor de chipkaart. Waarom? Omdat de creditcardmaatschappijen belang hebben bij het in stand houden van het systeem en daar vertrouwen voor nodig hebben. En daar doen ze hun stinkende best voor.

Dus bouwen creditkaartmaatschappijen slimme computersystemen die continu transacties scannen op frauduleuze patronen en die erg verdachte betalingen weigeren. Maar dat weigeren doen ze niet te snel, want je zult als Nederlandse klant maar net geland zijn in Brazilië en geld nodig hebben en dat wordt geweigerd. En dus glipt er wel eens een transactie tussendoor en daarvoor compenseren de creditcardmaatschappijen ruimhartig. En daarom werkt de creditcard.

Zo kan de chipkaart ook werken met de huidige encryptie. Een computersysteem checkt het in- en uitchecken en als iemand 23 minuten na inchecken in Vlissingen uitcheckt in Delfzijl dan is er wat mis met die kaart. Als de computer dat opmerkt maakt die een nieuwe chipkaart en stuurt die, met een beetje extra tegoed voor de moeite, op naar de rechtmatige eigenaar. En zo gauw de nieuwe chipkaart gebruikt wordt blokkeer je de oude: poortjes gaan niet meer open voor de fraudeur. Klaar.

Dat wil echter niet zeggen dat de chipkaart geen problemen meer heeft. Maar de huidige hype rondom encryptie vertroebelt het zicht daarop. Die problemen circuleren om één thema: gebruiksgemak.

VERBETERDE VEILIGHEID LEIDT AF VAN VERBETERD GEBRUIKSGEMAK

AANDACHT NAAR VERSCHILLENDE PARTIJEN OVER ELKAAR HEEN OM TE SPLEN MET TARIEVEN. Technisch kan dat namelijk met de chipkaart. Echter, je weet vooraf nauwelijks meer wat de reis je gaat kosten. Daarnaast, je krijgt niet simpelweg de goedkoopste reis, waarbij bijvoorbeeld twee enkeltjes in omgekeerde richting vanzelf een retourtje worden, een reisje in de daluren goedkoper of je keten door bus, trein en metro zo slim mogelijk wordt gecombineerd tot een laagste prijs. Vervolgens moet je straks bij de NS je kaartje aan de automaat op je chipkaart laden; niks simpelweg in- en uitchecken. De makers en beheerders hebben misschien wel een prikkel tot veiligheid, maar die tot gebruiksgemak lijkt nog ver te zoeken.

Er ligt een nogal somber scenario op de loer. En dat is niet dat alle promovendi in de technische natuurkunde straks gratis kunnen reizen. Of dat openbaar-vervoerreizigers grote sommen geld kwijtraken via hun chipkaart. Of dat de persoonlijke gegevens van elke

chipkaarthouder op straat liggen. Dat sombere scenario is dat veel extra belastinggeld in de verbetering van de veiligheid van de chipkaart wordt gestoken. Een ding dat de strippenkaart vervangt. Geld dat ook ergens anders in gestoken zou kunnen worden, bijvoorbeeld in beter openbaar vervoer. Een tweede onderdeel van dat scenario is dat veel aandacht gaat naar verbeterde veiligheid en dat leidt af van verbeterd gebruiksgemak.

Tijd dus voor een reality check. Wat is er aan de hand? Iemand met stevige technische kennis kan straks misschien uw chipkaart uit uw portemonnee klonen en het tegoed in de bus of iets anders openbaars.

Wat kunt u daartegen doen? Laat het tegoed op uw chipkaart niet automatisch aanvullen vanaf uw rekening (dan bent u maximaal 20 euro kwijt, een gestolen strippenkaart) en stop uw chipkaart in een aluminium hoesje in uw portemonnee. Gratis tip tussendoor: vervoerders laat vast van die aluminium hoesjes maken met een mooi logo er op. Waarom wordt dit geen probleem? De vervoerders hebben er belang bij dat u geen last heeft van dat mogelijke klonen. Want willen ze u in het openbaar vervoer, dan moet het betalingsmiddel u geen last bezorgen. En ze hebben belang bij het aanpakken van kloners. Want kloners creëren zwartrijders en dus minder inkomsten.

Wat ga ik zelf doen: ik reis met de chipkaart waar het kan, laat hem gewoon automatisch aanvullen vanaf mijn rekening en maak niet zelf een aluminium hoesje: ik wacht even op de mooiste die ik krijg opgestuurd.

Dat allemaal wilde ik gaan zeggen bij Nova. In de ongeveer 2 minuten die ze voor me hadden. Ik blijf een optimist. Nova belde opnieuw. Dat ze studio-gasten hadden bij een ander onderwerp. En dat de uitzending volstroomde. Maar dat ze er graag nog eens op terugkwamen. Ach, de chipkaart wordt vanzelf weer nieuws.