FACTSHEET FS-2008-03

Kwetsbaarheden Mifare Classic chips in toegangspassen

Sinds begin 2008 is in het nieuws en in de politiek veel aandacht besteed aan het 'gekraakt' zijn van de OV-chipkaart en toegangspassen voor gebouwen. De aanleiding van deze aandacht ligt in de elektronische chips die in beide gevallen wordt gebruikt: de Mifare Classic RFID chips. Wetenschappers hebben in deze chips kwetsbaarheden ontdekt waardoor de beveiliging ervan is te doorbreken zodat de gegevens op chipkaarten zijn uit te lezen en chipkaarten zijn te kopiëren. In oktober 2008 zijn alle onderzoeksdetails hieromtrent vrijgegeven en inmiddels is programmatuur waarmee chips daadwerkelijk kunnen worden gekraakt vrij verkrijgbaar.

Deze factsheet biedt nadere informatie over de ontdekte kwetsbaarheden en de gevolgen hiervan voor het gebruik in toegangssystemen. Allereerst wordt de werking van Mifare Classic chips beschreven. Vervolgens wordt ingegaan op de ontdekte kwetsbaarheden en hoe de beveiliging van de chips kan worden doorbroken. Aansluitend worden de gevolgen voor praktijktoepassingen van de chips beschreven. Tot slot worden maatregelen gegeven die kunnen worden getroffen om de risico's te beperken.

In oktober 2011 hebben onderzoekers ook de beveiliging doorbroken van een van de opvolgers van de 'classic' namelijk de DESfire MF3ICD40[1].

De belangrijkste feiten op een rij:

- Onderzoekers hebben de beveiliging doorbroken van Mifare Classic RFID chips die onder andere worden gebruikt in de OV-chipkaart en in toegangspassen.
- De ontdekte aanvalstechnieken hebben alleen betrekking op chips van het type Mifare Classic 1K, 4K en Mini.
- De doorbraak is mogelijk doordat de beveiliging van de chip is gebaseerd op een voorheen geheime versleutelings-methode, die bekend is geworden.
- In de implementatie van de versleutelings-methode blijken zwakheden te bestaan die het doorbreken van de beveiliging veel eenvoudiger maken.
- Het doorbreken van de beveiliging maakt het mogelijk gegevens van passen uit te lezen en vervolgens passen te kopiëren.
- De onderzoekers hebben op 6 oktober 2008 hun onderzoeksdetails gepubliceerd. Daardoor is bekend geworden hoe de beveiliging van Mifare Classic chips kan worden doorbroken.
- Inmiddels is er eerste kant-en-klare programmacode beschikbaar gekomen waarmee in combinatie met een RFID-lezer chips kunnen worden gekraakt.
- Gebruikers van Mifare chips in toegangs-systemen kunnen aanvullende maatregelen treffen om de risico's van misbruik te beperken.
- Op termijn overstappen naar nieuwe, beter beveiligde toegangspassen (en vaak ook paslezers) is in veel gevallen vereist om de risico's op lange termijn te kunnen afvangen.

De werking van Mifare Classic RFID chips

RFID chips (Radio Frequency Identification) zijn elektronische chips die contactloze uitwisseling van gegevens op korte afstand mogelijk maken tussen een chip en een leesapparaat. Het gebruik van deze chips is in de laatste vijftien jaar enorm toegenomen, mede doordat ze zo goedkoop zijn. Ze worden onder andere gebruikt in de logistiek en detailhandel, maar ook in toegangspassen voor gebouwen en transactiesystemen[2].

Eén van de meest gebruikte RFID chips is de Mifare Classic van NXP Semiconductors Van deze chip zijn volgens de fabrikant door de jaren heen meer dan één miljard chips verkocht[3].

De Mifare Classic chips beschikken over beveiligings-mechanismen om de opgeslagen gegevens te beschermen. Zo wordt de communicatie tussen een chip en een leesapparaat versleuteld. Ook controleren chips en leesapparatuur aan het begin van de communicatie elkaars betrouwbaarheid (wederzijdse authenticatie). De versleutelingsmethode (het encryptie-algoritme) die de Mifare Classic bij deze mechanismen gebruikt, wordt Crypto-1 genoemd. Dit algoritme is intellectueel eigendom van NXP Semiconductors en de werking ervan was tot voor kort niet publiek. Deze geheimhouding is onderdeel van de beoogde beveiliging van de chip.

1 Zie http://mifare.net/links/news/update-on-mifare-desfire-mf3icd40

2 Zie http://www.rfidnederland.nl/upload/bestanden/20070507_122444.pdf

3 Zie http://www.nxp.com/products/identification/mifare/classic/

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

Kwetsbaarheden in de beveiliging

Eind 2007 hebben Duitse onderzoekers bekend gemaakt dat zij de werking van het geheime Crypto-1 encryptie-algoritme van de Mifare Classic hebben ontrafeld[4]. Daarbij hebben zij, naast het al bekende gebruik van korte 48-bit sleutels, enkele zwakheden ontdekt in het algoritme en de wijze waarop het authenticatieprotocol is geïmplementeerd op de chip[5].

In navolging van de Duitse onderzoekers hebben onderzoekers van de Radboud Universiteit in Nijmegen op 12 maart 2008 bekend gemaakt dat zij daadwerkelijk in staat zijn om Mifare Classic chips te kraken en te kopiëren[6]. Met hun methode is het mogelijk de chips in enkele seconden te kraken met gangbare apparatuur. De resultaten zijn door de AIVD gevalideerd. Ook heeft het kabinet de Tweede Kamer geïnformeerd[7].

Op 6 oktober 2008 hebben de Radboud-onderzoekers de volledige details van hun onderzoek gepubliceerd[8]. Daarbij zijn geen nieuwe kwetsbaarheden bekend geworden, maar zijn wel de cryptografische details bekend gemaakt die ten grondslag liggen aan het kraken van de chips. Hierdoor kregen derden ook de mogelijkheid om programmatuur en hardware te ontwikkelen om de chips te kraken. 23 oktober 2008 is al de eerste programmatuur beschikbaar gekomen waarmee daadwerkelijk chips kunnen worden gekraakt[9]. Om deze programmatuur te kunnen gebruiken, moet deze worden gecombineerd met speciale RFID-apparatuur (bijvoorbeeld Proxmark of OpenPCD).

De gepubliceerde kwetsbaarheden hebben alleen betrekking op de Mifare Classic 1K, 4K en Mini chips en op het Mifare Classic gedeelte van kaarten die Mifare Classic emulatie aan boord hebben. Op het moment van schrijven zijn de typen Mifare 'Desfire' en 'Desfire8' niet kwetsbaar voor de ontwikkelde aanvalstechnieken. De Desfire8 chip gebruikt een publiekelijk bekend encryptie-algoritme (triple DES of AES) met een lange sleutel.. De beveiliging van de Mifare Desfire MF3ICD40 is in 2011 inmiddels ook gekraakt maar door een ander type aanval[10]. Van de Mifare Desfire8 (nu bekend als Desfire EV1) zijn op het moment van schrijven nog geen beveiligingsproblemen bekend.

In de media is ook aandacht besteed aan Mifare Ultralight chips, die gebruikt worden in dagkaarten van de OV-chipkaart. Deze chips zijn nauwelijks beveiligd en eenvoudig te kopiëren[11]. Dit is dus een andere chip dan de Mifare Classic. Deze chip wordt over het algemeen niet gebruikt om fysieke toegang tot gebouwen te beveiligen.

Verschllende typen Mifare chips

Type	Kwetsbaar?
> Mifare Ultralight	Ja*
> Mifare Classic 1K/4K/Mini	Ja
> Mifare Desfire/Desfire8	Nee**

- *De Mifare Ultralight bevat minder beveiliging dan de Mifare Classic en was daardoor al eerder op eenvoudige wijze te kopiëren.*
  ***De Mifare DESfire MF3ICD40 is inmiddels kwestbaar gebleken voor een andersoortige aanvals techniek.*

Het doorbreken van de beveiliging

Het doel van het kraken van Mifare Classic chips in toegangssystemen is om ongeautoriseerd toegang tot beveiligde omgevingen te krijgen. Dit is het meest eenvoudig wanneer de toegangsbeveiliging van een omgeving alleen is gebaseerd op het unieke nummer van een Mifare Classic chip, het UID. Dit UID wordt namelijk onversleuteld uitgewisseld tussen een pas en een paslezer. Dit betekent dat het mogelijk is de communicatie tussen een pas en een paslezer af te luisteren, het UID vast te stellen en vervolgens dit UID op een nieuwe pas te zetten. Met deze kopie-pas kan toegang tot de beveiligde omgeving worden gekregen. Toegangsverlening op basis van alleen UID wordt veelal toegepast in ruimte met een lage gevoeligheid, zoals parkeergarages.

Een veiligere vorm van toegangsbeveiliging met de Mifare Classic chip is via identificatiegegevens die versleuteld op de chip worden opgeslagen. Om een pas uit te lezen en te kopiëren moet deze versleuteling worden doorbroken. Dit kan door het afluisteren van de communicatie tussen een pas en een paslezer. Door het analyseren van deze communicatie kan de gebruikte sleutel worden

4 Zie http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
5 De zwakheden betreffen o.a. te grote lineariteit in de versleuteling en zwakheden in de random number generator.
6 Zie http://www.sos.cs.ru.nl/applications/rfid/persverklaring.pdf
7 Zie http://www.minbzk.nl/contents/pages/91905/briefaantweedekameroverchiptechnologietoegangs-passen.pdf
8 Zie http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf
9 Zie http://code.google.com/p/crapto1/
10 Zie http://mifare.net/links/news/update-on-mifare-desfire-mf3icd40
11 Zie https://ovchip.cs.ru.nl/images/1/15/Ru-report.pdf

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

achterhaald en toegang tot de gegevens op de pas worden verkregen[12]. Vervolgens kunnen de gegevens worden uitgelezen en op een nieuwe chip worden gezet. Deze kopie-chip is voor een chiplezer die geen verdere beveiligingscontroles uitvoert niet te onderscheiden van de originele chip.

Voor het afluisteren en ontcijferen van versleutelde communicatie tussen een pas en een paslezer bestaan in hoofdlijnen twee verschillende aanvalsscenario's:

1. *Afluisteren van communicatie tussen echte pas en een paslezer*
   Door eenmalig de communicatie van een echte pas en een echte paslezer (horend bij hetzelfde toegangssysteem) af te luisteren en deze vervolgens met een kraakprogramma te ontcijferen, kan de versleuteling worden doorbroken.

2. *Afluisteren van communicatie tussen een valse pas en een paslezer*
   De versleuteling kan ook worden doorbroken door twee maal de communicatie van een valse pas en een echte paslezer (niet horend bij hetzelfde toegangssysteem) af te luisteren en dit te ontcijferen. Deze methode heeft voor aanvallers het voordeel dat zij zelf met een valse pas het afluistermoment kunnen creëren. Ook is de geheime sleutel via deze methode sneller te ontcijferen.

Het is, gezien de recente snelle ontwikkelingen, niet ondenkbaar dat aanvallen ontdekt zullen worden waarbij alleen een echte pas voldoende is om sleutelmateriaal en data van deze pas af te lezen

Gevolgen voor praktijktoepassingen

De belangrijkste toepassingsgebieden van Mifare Classic chips zijn fysieke toegangssystemen en (micro)transactiesystemen. Zodra middelen beschikbaar komen om Mifare chips te kraken, is het reëel om aanvallen op deze toepassingen te verwachten. Zonder aanvullende maatregelen wordt het dan voor ongeautoriseerden mogelijk om met gekopieerde pasjes toegang te verkrijgen tot omgevingen die zijn beveiligd met een op Mifare Classic gebaseerd toegangssysteem.

De beveiliging van toegangscontrolesystemen die gebruik maken van Mifare technologie hangt echter vaak van meer factoren af dan alleen de chip zelf. De uiteindelijke impact hangt af van de aanvullende maatregelen die zijn getroffen in een toepassing. Bij aanvullende maatregelen kan het gaan om uiteenlopende zaken, zoals beveiliging met fysiek toezicht, additionele toegangscontrolemechanismen als PIN-codes of biometrie en procedures rondom uitgave, gebruik en inname van passen.

Welke maatregelen kunt u nemen om de risico's te beperken?

Gezien het risico dat toegangspassen op basis van de Mifare Classic gekraakt kunnen worden, raden wij u met nadruk aan om op korte termijn actie te ondernemen. De onderstaande stappen kunnen daarbij dienen als richtlijn:

- *Ga na of er binnen de organisatie toepassingen van de Mifare Classic chip bestaan*
  Om te bepalen welke risico's worden gelopen en of nadere actie vereist is, moet eerst worden bepaald of de Mifare Classic chip of een chip met Mifare Classic emulatie wordt gebruikt.
- *Bepaal de al getroffen beveiligingsmaatregelen;*
  Wanneer de standaardbeveiliging van de Mifare Classic als ineffectief wordt beschouwd, komt de beveiliging neer op de aanvullende maatregelen. Deze moeten daarom per toepassing worden geïnventariseerd, om de daadwerkelijke impact in uw eigen omgeving goed te kunnen bepalen.
- *Evalueer wat het resterende risico is en tref indien nodig aanvullende maatregelen.*
  Ga na of de getroffen maatregelen afdoende zijn, gezien de gevoeligheid van de beschermde omgevingen (die ook binnen één locatie kan verschillen). Kernvraag daarbij is: bieden de getroffen maatregelen voldoende beveiliging, gezien de schade die ongeautoriseerde toegang tot een omgeving kan hebben? Als de maatregelen onvoldoende zijn is het wenselijk extra maatregelen te treffen om de risico's te beperken. Zie het kader hieronder voor voorbeelden van maatregelen.

[12] Zie http://www.ru.nl/ds/research/rfid/

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

- *Overweeg vervanging van Mifare Classic chips door een betere variant.*
  Afhankelijk van het effect en de kosten van aanvullende maatregelen, kan het nodig zijn het vervangen van Mifare Classic chips door een betere variant te overwegen. Let daarbij op of de gebruikte paslezers, eventueel met een software-update, in staat zijn ook met complexere chips samen te werken. In dat geval hoeven alleen de passen fysiek te worden vervangen, wat minder kosten met zich mee brengt. Let wel: aangezien het vervangen van de chips vaak een langdurig traject zal is, is het (tijdelijk) treffen van aanvullende maatregelen onvermijdelijk.

  Alhoewel in 2008 de Mifare DESfire MF3ICD40 al niet meer actief verkocht werd door NXP bestaat de kans dat organisaties deze chip als vervanger ingevoerd hebben. Gezien de recente ontwikkelingen zult u deze chip op termijn ook moeten vervangen. Op dit moment vereist het kraken nog veel expertise en tijd maar de verwachting is dat deze inspanning in de toekomst zal afnemen.

Tot slot

Het is belangrijk te realiseren dat toegangssystemen die geen gebruik maken van de Mifare Classic chips mogelijk nog zwakker zijn dan de nu gekraakte systemen. Dit geldt vooral voor oudere systemen, die bijvoorbeeld nog gebruik maken van magneetstrips of communicatie zonder encryptie. Hoewel de huidige media-aandacht voor de Mifare Classic chips maakt dat de impact daarvan zeer groot kan zijn, mogen ook andere systemen in dit kader niet worden veronachtzaamd.

Mogelijke aanvullende beveiligingsmaatregelen

Dit zijn voorbeelden van maatregelen die u kunt treffen om de risico's van kwetsbare Mifare chips te beperken. De daadwerkelijk te treffen maatregelen zijn afhankelijk van uw specifieke toepassing. Als intern onvoldoende expertise op dit gebied beschikbaar is, is het aan te bevelen contact op te nemen met uw leverancier of een externe specialist.

Organisatorische maatregelen:

> Stel visuele controles in op passen bij toegangs-systemen (bijv. een gebouwingang), om te controleren op ongeautoriseerde toegangspogingen. Daarbij kan worden gelet op vormgeving van de pas, aanwezige pasfoto's en eventuele andere echtheidskenmerken.

> Voer draagplicht voor toegangspassen in. Vooral in grote organisaties, of locaties met veel externe medewerkers of bezoekers helpt draagplicht bij het identificeren van ongewenste aanwezigen.

> Verhoog het beveiligingsbewustzijn van medewerkers, door te communiceren over risico's en getroffen maatregelen. Het identificeren van risico's begint met het kennen van mogelijke risico's.

> Richt procedures in rondom uitgifte en inname van passen, om te voorkomen dat passen gaan zwerven of in handen van kwaadwillende terechtkomen. Besteed daarbij aandacht aan te ondernemen acties bij verlies of diefstal (zoals blokkade van passen).

> Scherp waar mogelijk toegangsrechten van passen aan, om de gevolgen van gekopieerde passen te beperken. Let daarbij in eerste instantie vooral op kritieke ruimten.

> Zorg dat procedures beschikbaar zijn voor het afhandelen en escaleren van meldingen van ongeautoriseerde toegang.

> Zorg voor strikte procedures rondom de ontvangst en begeleiding van bezoekers. Zorg daarbij dat inname van bezoekerspassen een vereiste is.

> Voer een controle en opschoning uit van uitgegeven toegangspassen. Blokkeer passen van vertrokken medewerkers.

> Let extra op verdachte personen die rondhangen bij paslezers, om pogingen tot het afvangen van communicatie te verhinderen.

Technische maatregelen:

> Vermijd bij voorkeur toegangscontrole op basis van alleen het UID van een chip.

> Beveilig passen niet allemaal op basis van dezelfde sleutel, maar maak gebruik van sleuteldiversificatie.

> Dwing indien mogelijk af dat het toegangssyteem passen op basis van het UID blokkeert na meerdere foutieve authenticatiepogingen.

> Sla transactietellers op, zowel in het toegangssyteem als in passen, zodat alleen sequentiële pogingen worden geaccepteerd. Dit helpt tegen het gebruik van kopie-passen, omdat in dat geval de doorlopende telling van transacties niet meer klopt.

> Activeer indien mogelijk 'anti-passback' functionaliteit in fysieke toegangssystemen. Dit houdt in dat wordt afgedwongen dat een pas niet twee keer achter elkaar toegang krijgt zonder tussentijds vertrek.

> Activeer, indien mogelijk, functionaliteit om ongeautoriseerde acties te identificeren. Een voorbeeld daarvan is het kort na elkaar aanbieden van een pas op twee ver uit elkaar gelegen locaties.

> Voer waar mogelijk twee-factor authenticatie in voor de meest kritieke ruimten. Bij twee-factor authenticatie wordt niet alleen het bezit van de pas gecontroleerd, maar bijvoorbeeld ook kennis van een pincode of een biometrische eigenschap zoals een vingerafdruk.

> Voorzie gebruikers van beschermende hoesjes die geen straling doorlaten. Door pasjes hierin te bewaren kunnen pasjes niet worden uitgelezen wanneer ze niet worden gebruikt. Dit voorkomt echter niet het afvangen van communicatie tijdens het gebruik van de pasjes.

> Deactiveer indien nodig kaartlezers en stap over op andere toegangscontroles (zoals centrale deurbediening of fysieke controle bij de deur).

GOVCERT.NL is het Cyber Security & Incident Response Team van de Nederlandse overheid. Vragen over de inhoud van deze factsheet kunt u richten aan info@govcert.nl of telefonisch via 070-8887555.