Persverklaring, Digital Security, Radboud Universiteit Nijmegen, 12 maart 2008

Ontmanteling contactloze chipkaart

Samenvatting

Vrijdag 7 maart 2008 hebben onderzoekers en studenten van de onderzoeksgroep Digital Security van de Radboud Universiteit Nijmegen een lek in de beveiliging van een veelgebruikt type contactloze chipkaart gevonden. Eerder hadden de Duitse wetenschappers Nohl en Plötz ook al op zwakheden gewezen. Het gaat hier om de zogenaamde "Mifare Classic" RFID-kaart die door NXP (voorheen Philips Semiconductors) geproduceerd wordt. Er zijn er wereldwijd ongeveer een miljard van verkocht.

Deze kaart wordt gebruikt voor de OV-chipkaart in Nederland en voor vergelijkbare openbaar vervoer toepassingen in het buitenland (zoals bijvoorbeeld de metro in Londen en Hong Kong). Ook wordt de Mifare Classic gebruikt in toegangspasjes voor de beveiliging van gebouwen en terreinen. Daardoor heeft dit lek een bredere impact. Doordat bepaalde kaarten gekloond kunnen worden, is het in principe mogelijk om onder een gestolen identiteit gebouwen en terreinen te betreden. Dit is in de praktijk aangetoond. In veel omstandigheden bestaan er echter aanvullende lagen van beveiliging. Het is dan ook raadzaam deze extra lagen te versterken.

De Digital Security groep heeft zwakheden in het authenticatiemechanisme van de Mifare Classic gevonden. Te weten:

1. De werking van het CRYPTO-1 algoritme is tot in detail achterhaald.
2. Er is een betrekkelijk eenvoudige manier gevonden om de benodigde cryptografische sleutels te achterhalen. Dure apparatuur is hiervoor niet vereist.

Door deze twee punten te combineren is een daadwerkelijke aanval uitgevoerd: een Mifare Classic toegangspas is succesvol gekloond. Op deze manier kan een kwaadwillende oneigenlijk toegang verkrijgen, wanneer aanvullende beveiligingsmaatregelen ontbreken.

Achtergrond

De Mifare Classic is een contactloze chipkaart die midden jaren 90 ontwikkeld is. Het

is een geheugenkaart met enige bescherming. De kaart is niet programmeerbaar. De cryptografische berekeningen zijn direct in de hardware vastgelegd, en worden uitgevoerd via een “schuifregister” (LFSR) en een “filterfunctie”. Het hierbij gebruikte algoritme heet CRYPTO-1 en is bedrijfsgeheim van NXP. De beveiliging van deze kaart is mede afhankelijk van het geheim houden van CRYPTO-1. Dit staat bekend als “security by obscurity”.

Deze kaarten worden veel gebruikt voor *authenticatie*. Hierbij gaat het erom dat twee partijen aan elkaar bewijzen wie ze zijn. Ze doen dat door beide aan elkaar te laten zien dat ze over geheime informatie beschikken in de vorm van een gedeelde cryptografische sleutel. Wanneer beide partijen (kaart en kaartlezer) bepaalde berekeningen uitvoeren en de uitkomsten van elkaar controleren, weten ze zeker met wie ze te doen hebben.

Authenticatie is nodig voor toegang tot gebouwen en terreinen. Daar worden deze kaarten veel voor gebruikt. Men spreekt dan van *access control*.

Succesvolle authenticatie is ook nodig om in het geheugen van de Mifare Classic te lezen of te schrijven. Het geheugen is verdeeld in verschillende sectoren. Iedere sector heeft in principe twee eigen sleutels.

Sleutelbeheer is een onderwerp apart. Er zijn ruwweg twee mogelijkheden.

1. Binnen een bepaalde toepassing hebben alle kaarten en kaartlezers dezelfde sleutel voor authenticatie (voor een bepaalde sector). Dit komt veel voor bij access control.
2. Iedere kaart heeft eigen sleutels. De kaartlezer moet dan eerst de kaart herkennen: de lezer kan dan de bijbehorende sleutels vinden of berekenen. Men spreekt van *diversified keys*. Dit wordt, naar verluidt, onder andere gebruikt bij de OV-chipkaart.

Zwakheden Mifare Classic

De Digital Security groep heeft zwakheden in het authenticatiemechanisme van de Mifare Classic gevonden. Te weten:

1. De werking van het CRYPTO-1 algoritme tot is in detail achterhaald. Op basis daarvan is een eigen implementatie van het algoritme gemaakt.
2. Er is een betrekkelijk eenvoudige manier gevonden om de benodigde cryptografische sleutels te achterhalen.

Voor het achterhalen van CRYPTO-1 is gebruik gemaakt van fouten in het authenticatieprotocol. Wanneer men zich niet netjes houdt aan het voorgeschreven

protocol voor communicatie, kan er informatie over de werking van het algoritme worden verkregen. Door die informatie op een geschikte manier te combineren bleek het algoritme te achterhalen.

Wanneer dit algoritme eenmaal bekend is kan men via een zogenaamde brute force methode alle mogelijkheden doorrekenen om een geheime sleutel te achterhalen. In deze situatie gaat het om cryptografische sleutels met een lengte van 48 bits. Daar is een uur of 9 voor nodig, met geavanceerde computers, zoals eerder vermeld in TNO-rapport 34643, “Security Analysis of the Dutch OV-Chipkaart” van 26 februari 2008.

Ook hier bleek echter dat bepaalde foutjes in het authenticatieprotocol uitgebuit konden worden. Hiermee komen we op het tweede punt: dit leidt tot een betrekkelijk eenvoudige methode om sleutels te achterhalen, zonder brute force. Men doet eerst een flink aantal authenticatiepogingen, die falen, maar wél enige informatie opleveren. Door de resultaten op te zoeken in een heel grote tabel, kan men een “hit” vinden, en daarbij de sleutel achterhalen. De tabel wordt éénmalig, van tevoren samengesteld door zelf het CRYPTO-1 algoritme vaak op specifieke input te laten draaien.

Bij de proof-of-concept aanval zijn veel authenticatiepogingen nodig tezamen met de genoemde grote tabel. Het opnemen van de authenticatiepogingen duurt een aantal uren. Dit kan heimelijk gebeuren met een verborgen antenne. Het ziet er naar uit dat de complexiteit dramatisch gereduceerd kan worden waardoor de aanval nog veel simpeler kan worden.

Exploitatie van de zwakheden.

Met behulp van de geheime cryptografische sleutel is misbruik mogelijk. De precieze mogelijkheden hangen sterk af van de situatie waarin de kaart gebruikt wordt. Een situatie die zeer kwetsbaar is, is bijvoorbeeld access control, zeker wanneer alle kaarten dezelfde sleutel hebben. Deze situatie komt voor bij toegangscontrole tot gebouwen en terreinen in de publieke en private sector. Een gedetailleerd overzicht hiervan is echter niet voorhanden.

In deze setting is een praktische aanval aangetoond, waarbij een kaart van bijvoorbeeld een werknemer gekloond kan worden, door simpelweg met een draagbare kaartlezer tegen die persoon op te botsen. De persoon van wie op deze manier de identiteit gestolen wordt, hoeft dat op dat moment niet eens te merken.

In een situatie met *diversified keys* is misbruik moeilijker, maar niet onmogelijk. Hiervan zijn nog geen praktische aanvallen uitgewerkt.

Tegenmaatregelen

Op technisch niveau zijn er op dit moment, binnen de Digital Security groep, geen tegenmaatregelen bekend. NXP geeft aan te denken dat tegenmaatregelen mogelijk zijn die het risico aanzienlijk beperken. Overleg daarover is gaande. Natuurlijk vermindert afscherming van pasjes, bijvoorbeeld in metalen houders, het risico op ongemerkt uitlezen van kaarten. Bij gebruik kunnen de kaarten echter alsnog uitgelezen worden, via een verstopte antenne naast de kaartlezer bij de toegangdeur.

Versterking van de traditionele/fysieke toegangscontrole is dus aan te raden. Sowieso zullen beter beveiligde objecten meerdere beveiligingslagen gebruiken, waarvan de chipkaart er slechts één is.

Duitse hackers

Eind december 2007 vertelden Karsten Nohl en Henryk Plötz op een hackerscongres in Berlijn dat ze CRYPTO-1 gereconstrueerd hadden. Hierop is voortgebouwd, waarbij er op de achtergrond enig onderling contact geweest is. Nohl en Plötz hebben het cruciale algoritme CRYPTO-1 echter voor zich gehouden. Zij voerden een zogenaamde “hardware attack” uit, waarbij zij de Mifare Classic chip laagje voor laagje ontleedden. Hun methode is volkomen verschillend van de bovenstaande methode, die gebaseerd is op cryptoanalytische exploitatie van zwakheden in het authenticatieprotocol.

Nohl en Plötz hebben geen praktische methode gedemonstreerd waarmee geheime sleutels te achterhalen zijn.

Openbaarmaking

Bij het ontdekken van beveiligingsproblemen ontstaat het dilemma hoe met deze kennis om te gaan. Bij directe publicatie kunnen belangen geschaad worden. Langdurige geheimhouding leidt doorgaans tot trage reacties waardoor misbruik lang mogelijk blijft. Het is gangbaar in de computer security community om beveiligingslekken na een korte vertraging bekend te maken, als redelijk evenwicht.

Ook deze aanpak is hier gevolgd. Op vrijdag 7 maart 2008 is de rijksoverheid ingelicht, omdat de staatsveiligheid hier mogelijk in het geding is. Op zaterdag 8

maart zijn medewerkers van het Nationaal Bureau voor Verbindingsbeveiliging (NBV, onderdeel van de AIVD) naar Nijmegen gekomen voor een assessment. De AIVD heeft vastgesteld dat de methode, zoals gedemonstreerd, werkt. Op zondag 9 maart is NXP gewaarschuwd, en op maandag 10 maart Trans Link Systems. Met medewerkers van beide organisaties zijn in Nijmegen de technische details besproken. Met hen wordt samengewerkt aan verdere analyse van de impact en van mogelijke tegenmaatregelen. Op woensdag 12 maart heeft minister Ter Horst de Tweede Kamer geïnformeerd.

Vanwege de gevoeligheid van de zaak worden technische details pas veel later, in overleg met de direct betrokkenen, openbaar gemaakt, en wel in reguliere wetenschappelijke publicaties.

De Digital Security groep

De Digital Security groep van de Radboud Universiteit Nijmegen bestaat uit ongeveer 25 onderzoekers. Het onderzoek richt zich op twee thema's: software security en identity-centric security. Chipkaarten zijn een onderwerp waarover de groep in de loop van de jaren grote expertise verzameld heeft. Zo heeft de groep geadviseerd over de technische aspecten van de chip in het biometrische paspoort. Ook is de groep onder andere aktief op het gebied van elektronisch stemmen, RFID, privacy en cybercrime. Voor meer informatie zie: http://www.ru.nl/ds

Meer informatie via de wetenschapsredactie van de Radboud Universiteit Nijmegen, tel. 024-3616000, email info@communicatie.ru.nl

medewerkers
ing. Ronny Wichers Schreur
dr. Peter van Rossum
drs. Flavio Garcia
dr. Wouter Teepe
dr. Jaap-Henk Hoepman
prof. dr. Bart Jacobs

studenten
ing. Gerhard de Koning Gans
ing. Roel Verdult
Ruben Muijrers
ing. Ravindra Kali
ing. Vinesh Kali