Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

23 645 Openbaar vervoer

Nr. 260

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 oktober 2008

Hierbij zend ik u de in de in de regeling van werkzaamheden van 28 oktober jl. door het lid Roemer (SP) gevraagde brief inzake nieuwe maatregelen naar aanleiding van het bericht dat de software van de OV-Chipkaart en deurpasjes te klonen openbaar is geworden. Ik zal ingaan op de vraag over eventuele extra te nemen maatregelen rond toegang tot overheidsgebouwen en namens de staatssecretaris van Verkeer en Waterstaat, op de mogelijke gevolgen voor de OV-chipkaart en welke stappen er ondernomen worden om misbruik van de OV-chipkaart te voorkomen.

OV-chipkaart

De beveiliging van de OV-chipkaart heeft de volle aandacht van de Staatssecretaris van Verkeer en Waterstaat. De afgelopen maanden zijn er daarom verschillende onderzoeken uitgevoerd om de risico's voor de OV-chipkaart in kaart te brengen. Er zijn maatregelen benoemd en genomen om de beveiliging van de OV-chipkaart op een dusdanig niveau te brengen dat deze geen bedreiging vormt voor het project an sich. Daadwerkelijke implementatie van de maatregelen worden intensief gemonitord door Royal Holloway University London. Tevens zal TLS periodieke rapportages over de hoogte van fraudelevels en daaraan gerelateerde bewegingen aanleveren.

Vooralsnog kan op basis van de op dit moment beschikbare informatie worden geconcludeerd dat publicatie van source code misbruik van de OV-chipkaart niet aantrekkelijker maakt en er niets veranderd is aan het feit dat de criminele business case negatief is en daarmee misbruik niet loont. TLS en de Vervoerders werken tegelijkertijd hard aan fraudebeheersing en continue verbetering daarvan, korte termijn maatregelen die het risico van misbruik met de mifare classic chip sterk verminderen, en een contingency-plan om te migreren naar een andere chip indien dit aan de orde mocht zijn.

KST123880
0809tkkst23645-260
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

De uitrol van de OV-chipkaart, door de decentrale overheden en vervoerders, zal op basis van deze informatie niet verder vertragen. Daarnaast heeft het Openbaar Ministerie de Staatssecretaris aangegeven direct op te treden indien daartoe aanleiding bestaat.

Toegangspassen

Ik heb kennisgenomen van het feit dat er «open source software» beschikbaar zou zijn die dupliceren van toegangspassen mogelijk maakt.
In een brief aan de Tweede Kamer van 22 september (31 700 VII, nr. 4) heb ik de Kamer laten weten dat de universiteit van Nijmegen in oktober op een congres in Spanje meer uitgebreid in zal gaan op de veiligheidsrisico's van de Mifare classic chip. Daarop heb ik aangegeven dat er vanaf dat moment sprake zou kunnen zijn van een groter risico. Daarvan zou nu sprake kunnen zijn. In diezelfde brief is een overzicht opgenomen van typen aanvullende maatregelen die genomen kunnen worden.

Consequenties voor gebruik Mifare Classic in toegangscontrole systemen

Met het publiceren van programma's voor het kraken van de Mifare Classic kaart wordt het risico groter dat onbevoegden zich toegang weten te verschaffen tot ruimtes beveiligd met toegangspassen gebaseerd op deze technologie. Dat dit nu gebeurt is niet verrassend; al in maart/april jl. is door het Nationaal Bureau voor Verbindingsbeveiliging van de AIVD erop gewezen dat na publicatie vrij snel kraakprogramma's op het internet beschikbaar zouden komen. Destijds is al nagegaan met de BVA's van de betrokken ministeries wat de tegenmaatregelen zouden kunnen zijn. Toen in juli jongstleden duidelijk werd dat publicatie zou gaan plaatsvinden, heeft AIVD/NBV de BVA's opnieuw hiervoor gewaarschuwd en zijn mogelijke (technische) tegenmaatregelen nader uitgewerkt.

Mogelijkheid van een Denial of Service aanval

Wanneer een aanvaller de beschikking heeft over bepaalde software om Mifare Classic kaarten aan te vallen, zijn er twee scenario's mogelijk die specifiek tot een Denial of Service kunnen leiden:
- Een valide kaart wordt gekloond, waarna de aanvaller zich met de gekloonde kaart aanmeldt bij het toegangscontrole systeem. Indien detectiemechanismen in de back-office van het toegangscontrole systeem zijn aangezet, is het voor de valide kaarthouder daarna niet meer mogelijk om zich toegang te verschaffen. Afhankelijk van het precieze scenario, is het mogelijk om deze aanval uit te voeren op één individuele kaart, of op een serie van kaarten tegelijk.
- Een valide kaart wordt door een aanvaller op afstand uitgelezen, waarna tevens aanpassingen in sectoren op de kaart kunnen worden gedaan (bijvoorbeeld het wissen van sleutelinformatie die nodig is voor de authenticatie). Hierdoor kan de kaart onbruikbaar worden gemaakt voor toegangscontrole: onklaargemaakte passen geven simpelweg geen toegang tot een pand.

Maatregelen tot invoering van de Rijkspas

Departementen die gebruikmaken van de Mifare classic chip in toegangspassen, hebben extra voorzieningen kunnen nemen om de huidige situatie te beheersen en kunnen bij toegenomen dreiging nog aanvullende maatregelen nemen. Het gaat hier om combinaties van technische en organisatorische maatregelen. Zo kan er meer visuele controle worden ingezet, door beveiligingsmedewerkers die fysiek aanwezig zijn bij ingangen van gebouwen. Procedures rond uitreiken van bezoekerskaarten

kunnen worden aangescherpt. Ook kan er meer aandacht worden besteed aan zichtbaar dragen van passen en begeleiden van bezoekers van en naar toegangsdeuren van het pand. Ook technisch kunnen er nog aanvullende maatregelen worden genomen. Zo kan de autorisatie verder worden beperkt, de verificatie verder worden uitgebreid met extra gegevens, passen worden voorzien van een kortere toegangsperiode en kunnen maatregelen worden genomen om de (heimelijke) uitleesbaarheid van passen verder te bemoeilijken. Ook kan er overgestapt worden op andere chiptechnologie. De departementen beschikken over een set van aanbevelingen over hoe te handelen.

Gebruik van anti-kopieer kaarthouders

Een belangrijke maatregel die zowel tegen het ongeautoriseerd toegang verschaffen als tegen een Denial of Service aanval (in beide scenario's) weerstand biedt, is het gebruik van zogenaamde RFID shields. Dit zijn anti-kopieer kaarthouders die het uitlezen van gevoelige informatie tegen kunnen gaan. AIVD/NBV heeft een bepaald type van deze kaarthouders onderzocht en geschikt bevonden om bescherming te bieden tegen ongewenst kopiëren. Momenteel zijn deze kaarthouders bij verschillende overheidsorganisaties reeds ingevoerd.

Mogelijke consequenties voor de Rijkspas ontwikkeling

Het bovenstaande betreft een tijdelijke situatie totdat een nieuwe chip beschikbaar is voor een nieuwe toegangspas, de Rijkspas. Ik ben voornemens om vanaf april volgend jaar de Rijkspas in te voeren, en rond de in die pas te hanteren chiptechnologie lopen een aantal beveiligingsonderzoeken.
Thans wordt de besluitvorming inzake de chipkeuze voorbereid. Bij deze keuze is naast functionaliteit voor toegangsverlening een adequaat beveiligingsniveau een belangrijke randvoorwaarde. De lopende onderzoeken van betrokken instanties naar de kandidaat chip(s) zijn erop gericht om het risico op klonen en/of Denial of Service aanvallen zo klein mogelijk te maken; de Mifare Classic technologie wordt in de Rijkspas derhalve niet meer gebruikt. Naast de beoogde beveiliging die de Rijkspas chip moet gaan bieden, is binnen de gehele keten van toegangscontrole systemen een aantal technische én organisatorische maatregelen in voorbereiding die het beveiligingsniveau verder moeten verhogen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst