Verslag overleg Halderwege CE.

MEMO

Aan: Michèle Blom (V&W), Keith Mayes (RHUL), Jasper Nillesen (V&W)
Van: Johan Knibbe (HEC)
Betreft: Short minutes of the RHUL interview on March 13th 2008 at V&W The Hague (final version)
C.c.:
Datum: March 25th 2008

Present: Michèle Blom, Keith Mayes, Jasper Nillesen, Johan Knibbe

Mayes gives an overview of the method of risk analyses used in the field of chipcard system security: to determine the effect of possible attacks by estimating their likelihood and impact. The different kinds of cipher (e.g. stream and block, public and proprietary) are briefly presented, as well as the role of the back office, the importance of key length and of the quality (real randomness) of the random generator. The counter expertise task is progressing well and according to plan. So far TLS and TNO have co-operated fully and have provided all requested documentation. Interviews have been scheduled with TLS and TNO to take place in Holland, whereas the majority of the counter expertise work is being carried out in England.

The Ministry representatives find the overview very useful and request a simple tutorial paper that can help non-technical people understand the main issues of the situation.

Blom points out that for the Ministry it is of utmost importance that the counter expertise be fully independent and based of professional integrity. If any problems might arise in the course of the counter expertise, HEC will assist, and the Ministry will give full support to solve them if needed. The resulting counter expertise report must be well readable for the general public, and make its points clearly so that there will be no misunderstanding about them.
In Parliament and press there is much attention for the subject. The Ministry of V&W and the Staatssecretaris are waiting for the counter expertise report before taking a position on the subject.

The procedure for delivering the report is confirmed by RHUL to be according to planning:

1. The draft of the findings will first be discussed by RHUL with TLS and TNO, which organisations will also have to agree formally on them not containing information falling under the NDA's. RHUL will provide TLS and TNO with technical information from its investigations that can be of interest for further analyses or developments.
2. The draft of the full public report will then be presented to the Ministry and HEC to test readability and clearness for the general public.
3. The final version of the counter expertise report will be delivered on or before Monday April 7th.

Commentaar op Concept KHLC rapport

Presentatie/bevindingen van de concept-contra expertise RHUL (London) op 4/4

1. Belangrijkste conclusies CEB:

- CEB is er van overtuigd dat de kaart feitelijk reeds volledig gekraakt is (reverse engineered).
- Bij veelvuldige fraudeaanvallen voldoen de back up maatregelen van het systeem waarschijnlijk niet meer, want ze zijn wellicht te bewerkelijk (qua bemensing, automatisering, reponssnelheid) om effect te hebben.
- De risico's van een landelijk operationele OV-chipkaart zijn groter dan aangenomen door TNO doordat er geen inzicht is in (a) de schaal waarin gekraakte chips worden gebruikt en (b) de effectiviteit van extra beveiligingsmaatregelen (in de backoffice).
- Technologische beveiligingsbarriéres van het systeem zijn niet (bewezen) bestand tegen de niet-onderzochte, maar wel al uitvoerbare aanvallen.
- Myfare Classic 4k chip zou moeten worden vervangen, zoals TNO ook suggereert. Want zo voegt de RHUL toe (blz, 5 en 6): 1) kaart steunt teveel op kwetsbaar en achterhaald beveiligingsalgoritme, 2) kraakapparatuur is gemakkelijk en relatief goedkoop te verkrijgen (trekt ook amateurkrakers aan), 3) kaart kan gemakkelijk worden gekopieerd, ook *the look and feel* (uiterlijk) van de kopie (kwaliteit is inspectieproof), 4) reizigers krijgen er last van als ze gekraakte tegoeden moeten terugvragen, waardoor vertrouwen in kaart (verder) kan dalen, 5) er kunnen valse claims van reizigers ontstaan. Laatstgenoemde 2 punten vallen onder secundaire effecten.
- Er is geen bewijs voor ondersteuning of verwerping van de door TNO geschatte 2 jaar termijn voor migratiegereedheid systeem. Datzelfde geldt voor de vraag of een big bang of geleidelijke migratie de beste keuze is, nu beveiligingsproblemen in omvang toenemen.
- Gezien het feit dat de werking (in termen van praktische toepasbaarheid) van de TNO maatregelen niet is aangetoond, en het waarschijnlijk flink energie zal kosten om ze nader uit te werken etc, wordt de vraag gesteld of het niet beter is die energie in plaats daarvan te richten op de keuze voor nieuwe chipkaarttechnologie.

2. Aanbevelingen

- Geadviseerd wordt daarom om een **tussentijdse milestone** aan het project toe te voegen voor januari 2009 die inhoudt dat naast de huidige uitrol naar een landelijk systeem van de OV-chipkaart, ook een compleet en gedetailleerd plan van de vervoersector gereed is over welke nieuwe technologie gebruikt zal gaan worden en wat daartoe stappen zijn ("complete plan how they would roll out an upgraded/migration solution"). Daarvoor is nodig, zo bleek bij de presentatie, dat de alle risico's en beheersmaatregelen in kaart zijn gebracht. Ook moet het plan voor uitrol door internationale experts zijn getoetst.
- Dat betekent concreet dat vóór ("prior to") die tussentijdse milestone stappen moeten zijn genomen, zoals: keuze nieuwe kaarttechnologie, inzet nieuwe of opgewaardeerde apparatuur/software, welke leveranciers, welke budgetten en planning van logistiek/distributie. Het onderliggende risicomanagement geeft aan wanneer (bijvoorbeeld bij aanvallen op systeem) je welke stappen moet nemen richting de gekozen oplossing.
- Inspanning wordt gericht op hoe een nieuwe (gekozen) kaarttechnologie en gemodificeerde kaartlezers stapsgewijs in bestaande systeem ingepast kunnen worden. Dit is volgens RHUL in theorie mogelijk.
- CEB adviseert m.b.t. de nieuwe chip een toekomstbestendig systeem. Dit impliceert twee zaken:
  - Kiezen voor een open-source encryptietechnologie, ipv van "geheim" algoritme.

- Modulair systeem waarbij algoritme van de chip losstaat van de rest van de infrastructuur zodat na verloop van tijd makkelijk kan worden overgeschakeld op (weer) een nieuwe encryptie en algoritme, zonder de overige infrastructurele communicatietechnologie.
- Er wordt aandacht gevraagd voor projectmanagement en risicomanagement

3. N.a.v. de presentatie/vragen

- [redacted]

4. Proces

- Het rapport is vrijdag 4 april door het RHUL aan HEC (Het Expertise Centrum, uitvoerend opdrachtgever) en VenW gepresenteerd. Zaterdag 5 april is er een bespreking met TLS over de presentatie.
- Op basis van presentatie aan VenW/HEC past RHUL de versie aan; deze gaat maandag 7 april naar HEC voor commentaar.
- Dinsdag ontvangt VenW het rapport met bevindingen van HEC.
- Vervolgens gaat rapport en bevinding naar Tweede Kamer, met voortgang proces richting besluitvorming.