From: Muller, F. (Frank)
Sent: Monday, November 24, 2008 1:58 PM
To: 'lia.gerritse-vanbavel@kpn.com'
Cc: Laarakkers, J. (Jeroen); E.Visscher@dvme.nl
Subject: RE: service based authentication
Attachments: RE: service based authentication

Hoi Lia,

De aanvraag voor service based authentication zou nu zo'n beetje af moeten zijn. Zie bijgevoegde mail van Erik van vorige week.

Groetjes,

Frank

From: lia.gerritse-vanbavel@kpn.com [mailto:lia.gerritse-vanbavel@kpn.com]
Sent: maandag 24 november 2008 9:45
To: Muller, F. (Frank); E.Visscher@dvme.nl
Cc: Laarakkers, J. (Jeroen)
Subject: RE: service based authentication

Heren,
Hoe gaat het hier nu mee? Ik zou deze toch wel graag binnenkort indienen, en als het even kan, nog eentje uit het RadioCards project in december. Gaat dat nog lukken?
Groetjes,
Lia

Van: Muller, F. (Frank) [mailto:frank.muller@tno.nl]
Verzonden: maandag 10 november 2008 19:56
Aan: Erik Visscher
CC: Laarakkers, J. (Jeroen); Gerritse, C.J. (Lia) (KPNCC L&R CIPO Intellectual Property)
Onderwerp: RE: service based authentication

Dag Erik,

Jouw tekst is zeer goed basismateriaal, maar zoals ik al schreef heeft het mij flink aan het denken gezet, wat een aantal nieuwe inzichten heeft opgeleverd.

Eerst maar even sec het commentaar op de huidige tekst. Hierbij een met Track Changes aangepaste versie van het Word document en licht aangepaste figuren. Ik heb wijzigingen gemaakt in de figuren 1, 3 en 4.

Nog de volgende aandachtspunten m.b.t. de figuren:

- De nummers 130 en 132 uit Figuur 1 komen niet terug in de tekst. Betekent dat, dat ze er uit kunnen, of dat een entiteit (b.v. de AC manager) dat nummer had moeten krijgen of hadden ze eigenlijk een ander

EX. 2021
Samsung v KPN
IPR2025-00512

nummer moeten hebben? Bijvoorbeeld nummer 128 uit de tekst komt weer niet voor in Figuur 1, terwijl dat misschien wel de bedoeling was.
- 312 en 314 komen nog niet correct voor in Figuur 3.

Zoals ik al in mijn vorige mail schreef, wordt het moeilijk om het AuC een eXpected Service Code door te geven of deze te laten bepalen door de Service Identification Unit in het AuC. Zo zijn er nog meer praktische bezwaren aan de uitvoeringsvoorbeelden zoals die er nu staan. Ik zou die echter wel laten staan, het zijn tenslotte voorbeelden.

Hieronder wordt nu het hele idee nog eens fundamenteler bekeken:

Eerst de requirements voor de oplossing:

- Een aanvaller mag de Service Code (SC) niet kunnen wijzigen; die moet dus hard in de respons vast zitten.
- Het HLR/AuC moet de waarde van de SC niet hoeven te kennen. In het interface naar het HLR/AuC zijn er namelijk geen mogelijkheden om deze door te geven; het HLR krijgt alleen de IMSI (International Mobile Subscriber Identity) van de gebruiker.
- Het HLR/AuC levert slechts één waarde voor XRES op aan de MSC/VLR, niet een reeks van uit te proberen uitkomsten. (Het interface biedt daar geen mogelijkheden voor.)
- Backwards compatibility: de oplossing moet ook werken met 'oude' Mobile Stations en MSC/VLR's die de SC niet meenemen in de berekening van de respons.
- Geen wijzigingen aan de (U)SIM. Dat er veranderingen aangebracht gaan worden aan de specs van SIM of USIM zien wij namelijk niet als een reeële optie.

Deze requirements leiden tot een oplossing waarbij niet het HLR/AuC een aanpassing maakt aan de respons, maar de MSC/VLR. Het AuC en de (U)SIM kunnen gewoon als vanouds blijven werken.

Dat betekent wel dat de geheime sleutel van de klant hier niet bij betrokken kan zijn, want die kennen alleen het AuC en de (U)SIM.

Dan kom ik er op uit dat er door het mobiel met de SC een wijziging van de response RES plaats moet vinden en wel met een one-way functie, zodat hij niet door de aanvaller ongedaan gemaakt kan worden. De MSC/VLR kan dezelfde one-way functie op de XRES en SC loslaten om de RES' te controleren. Dit heb ik (nog niet zo heel fraai) in een toegevoegde Figure 5 gezet. Eigenlijk staat deze oplossing in de grote lijn al wel beschreven op blz. 5, regel 30 tot blz 6, regel 18, maar moet als preferred uitvoeringsvoorbeeld worden toegevoegd, bovenaan (de huidige) blz. 16. Deze oplossing levert ook de gewenste backwards compatibility op: als het mobiel niet is voorzien van de mogelijkheid om de SC mee te nemen, doet de MSC/VLR dit ook niet, en vice versa.

Dit nieuwe gebeuren klopt m.i. nog precies met Claim 1 en Claim 2. Claim 3 en 4 zijn toegesneden op het door jou beschreven uitvoeringsvoorbeeld en gaan niet samen met de nieuwe inzichten. Dus ik denk dat er extra claims nodig zijn. De oude Claim 3 en 4 moeten wel blijven lijkt me. Claim 5, 6, 7, 8 en 9 passen ook op de nieuwe inzichten. Claim 10 weer niet. Claim 11 t/m 15 weer wel.

Verder zou er in het mobiel een Service Identification Unit (of Trusted Module, of Authentication Manager, of iets dergelijks) moeten zijn die veilig bepaalt via welk interface de challenge is binnengekomen en de juiste Service Code in de RES' verwerkt. Deze module zou ook de enige module mogen zijn die de waarde RES van de UICC ontvangt; zie mijn Figuur 6. De 3G radiocard zou deze rol kunnen spelen, maar dat hoeft niet.

Het enige dat nu nog niet helemaal goed beveiligd is, en waar ik nog even geen kant en klare oplossing voor heb, is dat de aanvaller het netwerk of het mobiel zich dommer voor zou kunnen laten doen dat het is (namelijk niet in staat om de SC mee te nemen in de response), en op die manier misbruik te maken van de backwards compatibility. Maar dat hoef ik toch niet al opgelost te hebben om op het idee tot dusver toch al patent te kunnen aanvragen?

Hier wilde ik het even bij laten. Kan je mij bellen als je er vragen over hebt, hetgeen ik me goed voor zou kunnen stellen, als ik meer gedetailleerde input moet leveren of als je wilt overleggen hoe we hiermee verder gaan?

Groeten,

Frank

From: Erik Visscher [mailto:E.Visscher@dvme.nl]
Sent: woensdag 8 oktober 2008 15:40
To: Laarakkers, J. (Jeroen)
Cc: Muller, F. (Frank); Hartog, T. (Tim); Fransen, F. (Frank); lia.gerritse-vanbavel@kpn.com
Subject: service based authentication

Beste allen,

Aangehecht de draft mbt bovengenoemde aanvrage. Graag kritsch commentaar en aanvullingen waar nodig. Ik had zelf ook nog een vraag (zie p.13 beschrijving).

Met vriendelijke groet,

De Vries & Metman
Erik Visscher

Overschiestraat 180
1062 XK Amsterdam
The Netherlands
Tel: +31 20 5110930
Fax: +31 20 5110931
E-mail general: mail@dvme.nl
Website: www.dvme.nl

This e-mail and the information it contains is for the use of the addressee(s) and may be confidential or privileged. Unauthorised use, disclosure or copying is strictly prohibited. If you are not the/an addressee and are in possession of this e-mail, please notify us immediately.

De Vries & Metman is a partnership consisting of professional corporations. The general terms and conditions of de Vries & Metman, which stipulate a limitation of liability, the applicability of Dutch law and the exclusive jurisdiction of the District Court of Amsterdam, are applicable to all work performed. A copy of the general terms and conditions is available on request or at www.dvme.nl.

This e-mail and its contents are subject to the DISCLAIMER at http://www.tno.nl/disclaimer/email.html