Minutes from meeting of GSMA/IETF experts on use of .gprs for IMS

Dear Colleagues,

Here is my summary of the major points from the conference call today (Sept 8, 2003) on the GSMA IREG proposal to use a *.gprs domain for resolving IMS identities synthesized from the IMSI. Please let me know of any errors or omissions. Also, please forward this to others that were on the call or are interested in the results as I could not understand everybody's names and do not have their e-mail addresses.

Issue to be addressed: The GSMA IREG has sent a LS to 3GPP requesting that it use a domain name ending in ".gprs" instead of ".3gppnetwork.org" as is currently in the 3GPP specifications. While this works technically, there have been objections raised within the IETF on use of TLDs that are not publicly registered. Specifically, the IETF was concerned that there would inevitably be leakage of these names into the internet. In the worst case situation of faulty clients, this could end up "hammering" the root DNS servers. The GSMA IREG felt that use of .gprs provided extra isolation and was desirable since GRX is a private network. It was also stated that each operator has contractual obligations to ensure that DNS queries are not "leaked" into the internet and if such leakage occurred it would be a severe security breach. It was unclear however what policing mechanisms existed outside of GRX to detect leakage.

Specific concerns about usage of "3gppnetwork.org":

1. The queries being discussed are synthesized from the user's IMSI and thus have secure information. It is critical that this not be leaked into the public internet. It was clarified that keeping queries out of the internet is completely dependent on where the DNS client (in this case a CSCF) routes its DNS query. If the query is routed to a DNS in the public internet, then security is breached regardless of whether the name to be resolved ends in ".gprs" or ".3gppnetwork.org". The 3GPP nodes must always route these queries to GRX DNS's. In fact, using ".3gppnetwork.org" it is possible to detect that such leakage is occurring by having a decoy host set up to receive these errant queries.

2. Hosts external to the GRX should not be able to make queries to the GRX DNS hosts. This issue is resolved by having different DNS resolution inside and outside of GRX. DNS queries for "*.3gppnetwork.org" arriving at a GRX DNS should be resolved in the usual manner. However outside of GRX (in the public internet), such queries could resolve to a decoy host that could log the external request and return an error message. This decoy host would in no way be connected to the GRX, but would simply act as a trap for requests outside of GRX. The public DNS would never know about the existence of GRX. This is a fairly standard DNS policy within corporate networks.

An alternate solution is to have .gprs accepted by ICANN as a public TLD, however, it was noted that the chances of success are low for this possibility.

Ultimately, it was agreed to withdraw the pending CR in 3GPP CN (N4-030932). Instead, Vodafone will introduce a new company sponsored CR

which keeps most aspects of the old CR, except for the .gprs TLD. In particular, Annex C (clarifying current construction of GPRS domain names) and the alternate string construction using mccxxx and mncxxx will also be retained. A LS will also be prepared for sending from 3GPP to GSMA IREG requesting that they incorporate "3gppnetwork.org" into the GRX DNS space. (Please note that a LS from 3GPP CN1 to GSMA SERG and IREG was already sent out in May 2002: http://www.3gpp.org/ftp/tsg_cn/WG1_mm-cc-sm/TSGN1_24/Docs/N1-021455.zip)

Thomas Narten can act as an informal contact for further communication between GSMA and IETF. Advice on the proper use of DNS can be obtained from the dnsop group (http://www.ietf.org/html.charters/dnsop-charter.html). Thomas can provide information on where to send formal LSs if they are needed.

Hope this captures the main points. Thanks again for a very productive conference call.

Stephen Hayes
3GPP TSG-CN Chair
Ericsson Inc.
Tel: +1 972 583 5773
Fax: +1 801 409 6319
Mobile: +1 469 360 8500
mailto:stephen.hayes@ericsson.com