

Important problems of IMS:

From Gunnar Heine

Translation of an article of German FUNKSCHAU magazine of April

In the following, significant problems of IMS will be discussed. We start with a repetition of the difficulties mentioned before.

Problem 1: Incoming calls
In accordance with 3GPP, until today the specifications regarding, how IMS-members can be accessed for regular telephone calls from the PSTN, are still missing. This point will be discussed in this article. The reason is, besides the inclusion of IMS in the expansion of the existing mobile-network: calls from the PSTN are accepted in the usual way through the network architecture. Later, the question about an IMS-involvement will be asked. We will write a following article about a method of resolution in the next edition.

Problem 2: Availability of real-time QoS in Access Networks (IP-CAN)
This problem is also described in the context to this article. It has a close connection with the problem 4 which is narrated below.

Problem 3: Interoperability
As demonstrated, there are problems with IMS-implementation in the interworking of terminals with the other terminal equipments and among themselves. The reasons for this are on one hand

the different IMS-standard alternatives and on the other hand the tendency to develop a system even before the standard is fully completed. Especially the last mentioned point is related to proprietary problem solving which leads to the mentioned interoperability problems when they will be in service.

Problem 4: Access from every access network
At least in the Release 5 version of 3GPP-standards the access to IMS is only possible from the GSM/GPRS- or UMTS-network. Indeed with Release 6, the access from alternative access technologies is possible, but these have to be so-called I-WLANs, in terms of 3GPP specifications. The reasons for this are the security concern and the above mentioned points under the problems 2, 5 and 6.

Problem 4a: NAT/NAPT
The topic NAT/NAPT needs to be mentioned as another handicap for the release of every type of access network. The use of private IP-addresses in the IMS-environment without complex methods at the network border is not possible, because SIP and especially SDP work with

embedded IP-addresses and port-numbers. In the next edition, we will pay most attention to this issue.

Problem 5: The possibility of "Intrusion" and DoS-attacks
The nightmares of every Telecom network provider are hackers. So far, Telecom providers were spared from these dangers in most cases, simply because the Telecom networks are not IP-networks. Certainly this will change with the mass production of IMS or, to express in common, with the migration to IP-based technique.

In this context, we can realise as one of the certain issues is the area of DoS-attacks. Generally the DoS-attack consist of the fact that there are so many requests send to the server that it has to quit the service or become unavailable for the "general" clients any longer because it cannot cope with the demands. This problem occurs when a server needs to reserve processor's output and capacity of the memory for every single request, whereas all these resources are naturally limited.

DoS-attacks in the IMS-area of 3GPP-networks are extremely pernicious because they can hit the mobile-network's heart immediately, precisely the HLR or HSS. So the entire service of a network can be brought to a standstill situation, not only the IMS. *Figure 4* illustrates the way of such an attack. Here it is important that according to 3PPP, only during the registration the system will switch over to an IPsec-tunnel. But the "default" SIP-Port 5060 of IMS or the P-CSCF is available for each correct formatted and received SIP: REGISTER-message. Each of these messages needs to be processed; this means it has to be passed on to the I-CSCF. If even there is a correct formatted IMPU (User-ID) present in the SIP: REGISTER, still the request has to be sent to one of the HLR's or HSS's. So the hacker brought up the greatest possible damage.

Now the question is asked why it is not possible to identify or address this problem at 3GPP immediately. The explanation lies in the history of IMS which is being mentioned. The problem of DoS-attacks exists when the access from any access network is provided, especially from WLAN or DSL-based network without authentication control.

As long as the access with GSM/GPRS- and UMTS-network is limited, the risk stays manageable, because these networks use a dedicated and composite access control. In the next edition, we will describe a possible method of resolution.

However the whole scenario becomes immediately unsafe as soon as the other types of operators and other types of clients or end terminals want to use IMS (keyword: Fixed Mobile Convergence). Thinking about the consequences that if from now

Version 6 for all IMS-users. This refers to the fact that, with IPv6 there will be availability of many addresses so that NAT/NAPT is not necessary any more and therefore the appropriate problems are just not well placed or set. Although this exception is correct, we want to point out to the inherent firewall-function of NAT/NAPT-routers, which should never be ignored. Due to this and many other reasons, 3GPP finally has to soften its MUST-demand to IPv6 again. For many manufacturers the situation today shows that the end equipment has to be provided with so-called dual-Stacks IPv4 / IPv6 to be compatible with every environment.

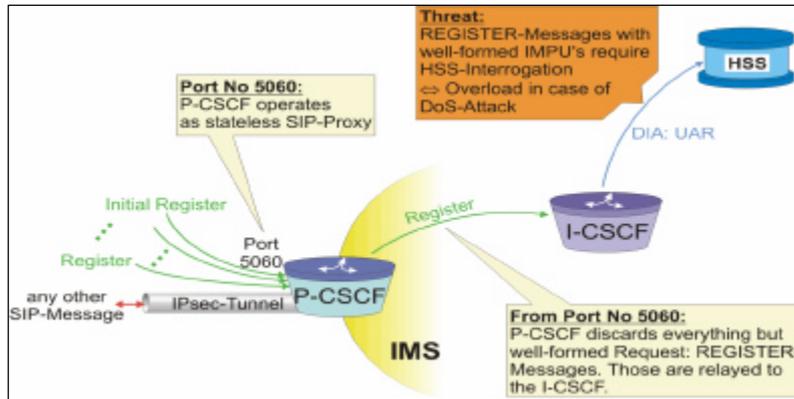


Figure 4: DoS-Attacke on IMS and HSS

Problem 6: Identification and authentication of the end user or the end terminal
 Again the problem is located in the history. The IMS-standardisation within 3GPP can be supported as the basic achievement of ETSI or GSM. Think about the necessary use of "Smart Cards" (SIM, USIM) at the end users for the purpose of identification and authentication. So far, this demand of hard cards has addressed the security-problem within the boundaries of GSM-based mobile-network.

on every landline-phone and every computer with "Softphone" -application requires a "Smart Card". Such a request cannot be realised. Also there is no concrete resolution method beyond the User-ID / Password or certificate-based attempts.

Problem 7: Which IP-addresses-version should be used (IPv4 or IPv6)
 The last topic is the problem with the IP-addresses. Certainly the difficulty with NAT and NAPT in 3GPP could have been seen before and now with the mandatory regulation for the use of IP-addresses of

RESULT:

Currently, the IMS as an open service platform is the most promising technical development in the area of NGN, VoIP and Triple-Play-Services. In this article, technology and history of IMS were defined shortly as well as different problems, which can be identified today. In the next edition as continuity, we will try to work on the ways of resolution for these problems and try to imagine the chances of these resolutions.