Abstract - Current research work of PhD student Charlott Eliasson, BTH

The IP Multimedia Subsystem (IMS) is regarded as one of the most prominent enablers for successful service provisioning across different access network technologies and devices. While new paradigms, e.g. seamless communication, enter the IMS, existing solutions, e.g. for authentication, need to be redefined, which is one of the major activities within the EUREKA!-funded Mobicome project, involving operators, manufacturers and academia. As there exist several candidate solutions for providing seamless authentication, there is a need for a set of criteria that helps to select the candidate that fulfils those criteria in a best possible way.

Given this background, a framework of criteria was proposed for the evaluation of authentication schemes in IMS. The primary criteria are security, user-friendliness and simplicity.
Security in the context of IMS authentication is defined as the level of security that is obtained for the user and the system when using a certain authentication scheme.
User-friendliness is defined as the probability that a typical user is able to authenticate without extra help or guidance. Furthermore, the user-perceived quality or Quality of Experience (QoE) for a user during the (TISPAN) authentication is also a measure of user-friendliness.
In the context of what the authentication scheme adds to the system, the authentication solution should be as simple as possible and still be sufficient as an authentication scheme. If the latter adds complexity to the system, the level of simplicity decreases. Simplicity is also closely related to scalability, in terms of effort and overhead.
In between these three criteria, the secondary criteria can be found. These are awareness, usability and algorithms. Each criterion, both primary and secondary, is then also divided into one or several substantiating sub-criteria.

The discussion of the criteria will be followed by a description of the evaluation methodology, which comprises both qualitative and quantitative evaluations such as SWOT analysis, use of NIST and ISO guidelines, user rankings, and measurements of authentication times.
The evaluation has been started with a SWOT analysis and user rankings. The latter is presently being applied in a user experiment, where the login will be delayed and the user will rank the experience. The Mean Opinion Score (MOS) will be used for the ranking and results.
The expected outcome of this experiment is that users react in the same manner when logging on to a website as when browsing an ordinary website that does not require the user to log on. This expectation is based on the input from users in a pre-evaluation of the experiment that was conducted at Dreamhack Winter 2008. The evaluation gave the impression that users do not have a different attitude towards waiting for a webpage containing authentication (login) than for a webpage that does not. The major problems seem to be related to scalability, meaning that users have so many accounts, for example on different communities, that it is not feasible for them to care about security anymore. Consequently, many users' attitude towards security in digital information and communication services can be considered jaded, eventually reaching a level of ignorance, but security is still needed. A user that for example is hacked will start care there and then. This would conclude that a security solution, ultimately, does not make life difficult for the user, but still protects him/her.

The presentation will be concluded with an outlook on future work, including future studies and experiments.