Evaluation of authentication schemes based on security, user-friendliness and complexity

Charlott Eliasson*, Markus Fiedler* and Ivar Jørstad**
* Blekinge Institute of Technology, Karlskrona, Sweden, {charlott.eliasson | markus.fiedler}@bth.se
** Ubisafe AS, Oslo, Norway, ivar@ubisafe.no

***Index Terms* — IMS security, seamless authentication, evaluation criteria.**

I. Introduction

In this work we are going to study and evaluate several SIM-based and non SIM-based authentication schemes for use in an IMS platform. The work will be done as part of the EUREKA!-funded Mobicome project [1]. In this project eleven partners are participating in order to get a working prototype of the new generation network IMS to run. The major idea of the extended IMS functionality is seamlessness, both regarding network and device switching. Seamlessly working security solutions are a self-evident must in this context. In order to satisfy the customer while meeting technical boundary conditions, solutions must work in a satisfactory manner in many respects.

On this background, this paper is a position paper, stating started and planned work on the evaluation of candidate security solutions for seamless IMS-based communications. First, the primary criteria of evaluation, namely security, user-friendliness and simplicity, are discussed. Then, the secondary criteria, which include awareness, usability and algorithms, are described. Along with the criteria, both sub-criteria and corresponding parameters are outlined. After this, the methodology for the evaluation is described. Finally, an outlook is presented at the end of the chapter.

II. Primary criteria

A. Security

This document defines security in the context of IMS authentication as the level of security that is obtained for the user and the system when using a certain authentication scheme. The following sub-criteria are considered: *authentication level*, (*automatic*) *trust with possible timeout and re-authentication*, and *known attacks*.

B. User-friendliness

We define the user-friendliness as how probable it is that a typical user is able to authenticate without extra help or guidance. Furthermore, the Quality of Experience (QoE) for a user during the (TISPAN) authentication is also a measure of user-friendliness. The user-friendliness might be low if the authentication takes too long or if the user does not fully understand *what* he or she is doing or *how* to do it. The latter is closely related to usability. The following sub-criteria are considered: *end-user experience*, *authentication time*, *password difficulty* and *functionality*.

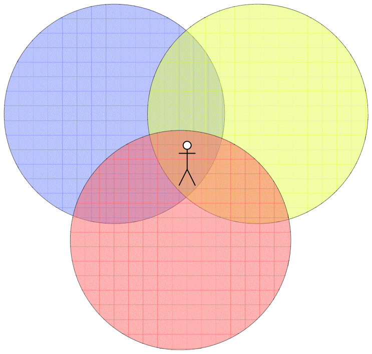

Fig. 1. Relationship between criteria.

C. Simplicity

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 closely related to scalability, in terms of effort and overhead. The following sub-criteria are considered: *execution time/speed*, *performance impact on system* and *performance impact on user equipment* (UE).

III. Secondary criteria

Interesting so-called secondary criteria are found at the intersections between the primary criteria discussed above, which is illustrated in Fig. 1.

A. Awareness

Awareness of the security service can be found as a criterion in the intersection between user-friendliness and security (see Fig. 1). The user can be aware of a service or application in a good or bad way. The good way can in this case be that the user feels secure. This can of course be a false feeling if the user feels secure beyond the authentication. There can also be false negative feedback, which is not as critical, as this will not harm the user or his integrity. Bad awareness can be caused by permanent and annoying positive feedback (e.g. a green light). The following sub-criteria are considered: *positive awareness*, *negative awareness*, *understanding* and *feedback*.

B. *Usability*

User-friendliness and simplicity together form the usability of a service (see Fig. 1). Usability is a concept that tells how well a user actually can use a service or application. It should be easy enough to be used by a typical user, but it should also have enough functionality. We define usability within this study as the ability for a typical user to use the scheme, based on how the scheme acts. This is closely connected to user-friendliness, but also to simplicity. If the scheme is complex and adds a huge execution time to the authentication process, then the user might not be able or willing to use it as intended. It also increases the risk of authentication failure. The following sub-criteria are considered: *effectiveness*, *efficiency* and *satisfaction*.

C. *Algorithms*

The simplicity and the security of a service are both based on the algorithm (see Fig. 1). This criterion is related to how the algorithm handles the task and how well they comply with each other. Both algorithms and the task are by themselves related to both security and simplicity. A complex algorithm should provide a higher level of security and a less complex algorithm (that might be needed in some cases) should provide a level of security that is as high as possible, given the level of complexity. *Providing security according to complexity* serves as sub-criterion.

IV. Methodology

In this section, the methodology of the evaluation is discussed. An outline of the methodology can be seen in Fig. 2, and each part will be explained in this chapter. To the left in Fig. 2, the rather qualitative methods can be found, and to the right, the rather quantitative methods are located. We will apply the criteria discussed in previous chapters.

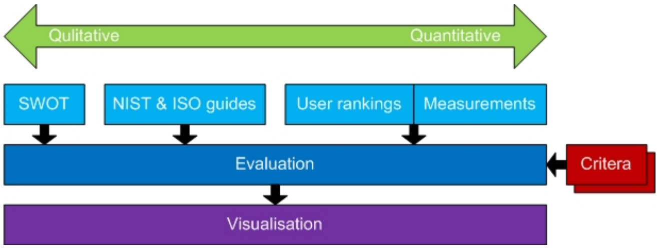

Fig. 2. Methodology of authentication scheme evaluation.

A. *SWOT*

Regarding the evaluation, there will first be a theoretical and conceptual investigation of the previously mentioned authentication schemes using SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. All known and documented aspects will be considered and the outcome will be a first judgement of each authentication scheme.

B. *NIST & ISO guidelines*

The authentication level will be evaluated conceptually, since it is based on what mechanisms are used in the scheme. The NIST [2] Electronic Guideline on Information Security [3] will be used as reference material, but the Common Criteria (CC) [4] will have the most significant role. A Protection Profile (PP) that suits IMS authentication will also be made or hopefully remade from an already matching PP, as a part of the CC process of producing a thoroughly evaluated product. CC is commonly used as part of a certifying process.

C. *User rankings*

The aspects of user-friendliness, awareness and usability can be evaluated “on top of” the IMS environment with real users, where their reactions are considered as subjective results. The user reactions will be documented through observations and also by users giving their subjective judgements of performed tasks. The user judgements can be given according to the MOS-scale, (1/worst – 5/best), which can then be compared to response times for the same tasks. Moreover, well-recognised results such as the ones reported in [5] can be taken into account.

D. *Measurements in a real IMS environment*

The aspects of security, simplicity and algorithms can be evaluated in a real IMS environment. The latter can be complemented with instruments in order to obtain objective results through measurements. Wiretaps and measurement points can be installed in the IMS environment in order to perform and control the traffic measurements.

V. Outlook

The next step that will be taken is to evaluate the authentication schemes in a web-based solution that will work more or less like a IMS environment, regarding authentication. As outlined above, this system will have several wiretaps deployed in strategic locations that will tell us how different parts of the system will respond to the different schemes.

The next steps that will be taken are the implementation of some target solutions and use of the methodologies mentioned above in order to evaluate the target solutions. As work proceeds, we also anticipate the need for a refinement of the above criteria.

References

[1] The Mobicome homepage [Online] [Cited: October 10, 2008.] http://www.mobicome.org.

[2] National Institute of Standards and Technology. [Online] [Cited: August 15, 2008.] http://www.nist.gov.

[3] Electronic Authentication Guideline. [Online] [Cited: August 15, 2008.] http://csrc.nist.gov/publications/drafts/800-63-1/Draft_SP-800-63-1_2008Feb20.pdf.

[4] Common Criteria. [Online] [Cited: October 10, 2008] http://www.commoncriteriaportal.org/

[5] J. Nielsen. Usability Engineering. Morgan Kaufman, San Francisco, 1994.