

Research in Progress

Mobile Communications Security Research at CSIR-MDS

Anna BAdimo & Fisseha Mekuria (PhD.)

Competency Area Manager Principal Research Scientist

abadimo@csir.co.za

fmekuria@csir.co.za

CSIR Modelling & Digital Sciences, Information Security Unit

CSIR Pretoria 0001, South Africa

Abstract:

The explosive growth of mobile communications technology and services in emerging markets has resulted that access to information resources and storage of sensitive information using mobile phones is increasing. At the same time the capabilities of mobile terminals and bandwidth of mobile networks is improving. To protect the information stored in mobile phones and to make it possible for mobile phone owners to utilize the vast amount of different mobile ICT services, it is important that security mechanisms with scalable encryption and authentication keys is available. The need for such security mechanisms is increasing proportionally with the explosive growth in mobile wireless communications. South Africa as one of the progressive emerging markets needs to address mobile security issues with the aim to develop the mobile enterprise and consumer services sector. Therefore CSIR modelling and digital sciences department, as a main stakeholder in the mobile ICT technologies and services in South Africa, have started a mobile communications security research group in collaboration with research institutes locally and abroad.

This paper will present the case study for and the proposed mobile communications security research. The mobile security research is based on several years of work in mobile wireless communications area and is composed of three parts:

- **Secure mobile terminal platforms:** Mobile data security and low power encryption and authentication mechanisms.
- **Next generation mobile wireless network security:** Radio access and handover security. (MS ↔ BTS,APs), and End-to-end security issues.
- **Secure Mobile Services :** Scalable security architectures for the vast amount of mobile services expected.

The research proposal also encompasses a human capital development aspect where several research proposals in collaboration with research universities and institutes, is expected to result in several research PhDs and the development of research and educational curriculum in the areas of mobile wireless communications security. The idea with this paper is to highlight and promote awareness to mobile-wireless security research and promote formation of collaborative research projects with research institutes in South Africa. The following section discusses one of the areas that the group at the CSIR is currently involved in. The research effort is focused to build a scalable platform to make mobile services secure and usable.

Research in Progress I:

A Scalable Platform for Secure Mobile Services

Nowadays mobile phone users are able to access a large number of services requiring some form of authentication. Making mobile services reliable is possible only by building security and authentication mechanisms, so that confidence and trust is built between service providers and customers. At the same time secure mobile services reduce fraudulent and unauthorized access to mobile broadband content and services, promoting the continued growth of mobile broadband technology and services. Secure mobile services require the development of security aware mobile platforms and network protocols. Depending on the type of services on demand the dimensions and rigor of security mechanisms can vary. As shown in figure 1 below, mobile services such as financial transactions (M-Banking, M-Payment) and mobile enterprise services will require high security, while public information access such as an M-E-Government application might need a low security level. Another important aspect that needs research is the interplay between strong/low security and less/better usability aspect of mobile services.

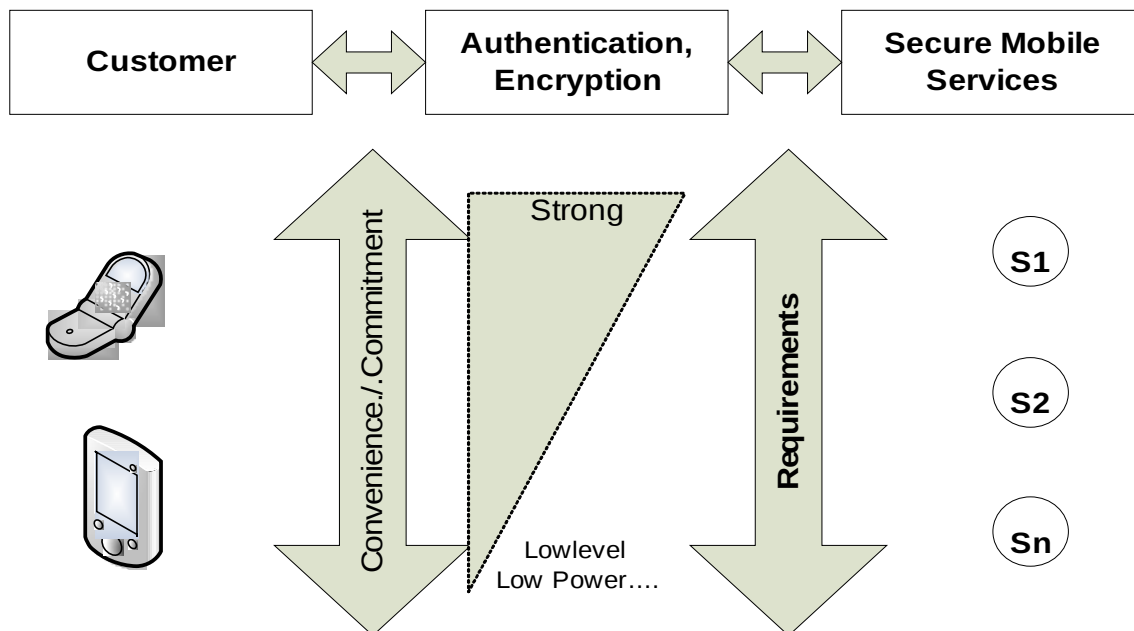


Figure 1, Security Dimensions of Mobile Broadband Services

References:

- 1- 3GPP Technical Specification: "Generic Authentication Architecture." 3GPP TS 33.222, 2007.
- 2- ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional Architecture", ETSI ES 282 007 V1.1.1, March 2006.
- 3- F. Mekuria, I.Rai "Issues in Next Generation Wireless Network Technologies & Services for Developing Regions", Proc. of Mobicom-08, WiNS-DR, Sept. 15-19,2008, San Francisco, USA.
- 4- Lu et.al., "A secure and Service-oriented Network Control Framework for WIMAX Networks.", IEEE Communications Magazine, Vol, 45, May 2007.