



## **ADAPTIVE AUTHENTICATION AND REGISTRATION KEY MANAGEMENT SCHEME BASED ON AAA ARCHITECTURE\***

**JONG-HYOUK LEE<sup>1,4</sup>, MOONSEONG KIM<sup>2</sup>, BYOUNG-SOO KOH<sup>3</sup>,  
AND TAI-MYOUNG CHUNG<sup>4</sup>**

<sup>1</sup>*IMARA Team*

*The French National Institute for Research in Computer Science and Control (INRIA)  
France*

*jong-hyouk.lee@inria.fr*

<sup>2</sup>*Korean Intellectual Property Office (KIPO)*

*Korea*

*moonseong@kipo.go.kr*

<sup>3</sup>*DigiCAPS Co., Ltd*

*Korea*

*bskoh@digicaps.com*

<sup>4</sup>*Internet Management Technology Laboratory*

*Sungkyunkwan University*

*Korea*

*{jhlee, tmchung}@imtl.skku.ac.kr*

**ABSTRACT**—The demand for mobile communications has been increasing significantly while inducing more challenges to security issues, especially in authenticating mobile hosts. In order to provide secure communications in mobile networks, the Authentication, Authorization, and Accounting (AAA) architecture is currently in use within the Internet access service. The AAA architecture is used to establish authentication between the communication hosts. However, the current architecture has an inefficient authentication procedure when a mobile host hands off from a home domain to foreign domains because the architecture assumes that the only reliable source of authenticating the mobile host is the AAA server located in the home domain. This problem becomes more significant when the mobile host traveling far way from its home domain establishes a mobility security association with mobility entities. To solve these problems, we propose in this paper an adaptive authentication and registration key management scheme. Within the proposed scheme, the mobile host is authenticated by the AAA server located in the previous domain and obtains the required key material to establish the mobility security association when the mobile host performs the inter-domain handoff. In the intra-domain handoff case, the mobile host is simply authenticated by the AAA server located in the current domain and obtains the required key material. The results of a performance evaluation show that the proposed scheme reduces the authentication failure rate up to 58.46% compared to the current AAA architecture.