ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 1, January 2015

End-To-End Secure Transmission of SMS Using EASYSMS Protocol

HANITHA. A[1], ZINNIAH.F[2],AGNES JOSHY.S[3]
Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[1]
Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[1]
Assistant Professor, Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[2]

Abstract— Nowadays, short message service (SMS) is being used in many daily life applications, including healthcare monitoring, Mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. In this paper, we propose an efficient and secure protocol called EasySMS, which provides end-to- end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. The analysis of the proposed protocol shows that this protocol is able to prevent various attacks, including SMS disclosure, over the air modification, replay attack, man-in-the- middle attack, and impersonation attack. The EasySMS protocol generates minimum communication and computation overheads as compared with existing SMSSec and PK-SIM protocols. On an average, the EasySMS protocol reduces 51% and 31% of the bandwidth consumption and reduces 62% and 45% of message exchanged during the authentication process in comparison to SMSSec and PK-SIM protocols respectively. Authors claim that EasySMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of cellular network.

Index Terms— Authentication, over-the-air, security, SMS, symmetric key.