International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **9**, September **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5353–5362

A SECURE E-MAIL PROTOCOL FOR MOBILE DEVICES

Chin-Chen Chang[1,2] and Chia-Yin Lee[2]

[1]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wen-Hwa Road, Xitun, Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chung Cheng University
No. 168, University Road, Minxiong, Chiayi 62102, Taiwan
{ ccc; licy }@cs.ccu.edu.tw

Received May 2010; revised September 2010

Abstract. *Electronic mail (e-mail) is one of the most important and widely-used applications for network environments. In recent years, e-mail has become a popular medium for various types of data transmission. The Pretty Good Privacy (PGP) program is one solution that ensures the confidentiality of e-mail. Unfortunately, PGP does not provide the secure requirement of perfect forward secrecy for e-mail. Recently, many secure e-mail protocols have been proposed to overcome this potential drawback of PGP. In this article, we point out some other potential drawbacks of existing protocols and propose a feasible, efficient e-mail protocol for mobile devices.*
Keywords: E-mail, Perfect forward secrecy, Man-in-the-middle attack, Mobile devices

1. **Introduction.** With the explosive growth of Internet applications, electronic mail (e-mail) has become a popular medium for data transmission. Since multimedia documents have already replaced the traditional text document, e-mail systems now transfer text as well as audio, video and graphics. Recently, the infrastructure for wireless networks has been developed extensively. Wireless networks serve the same purpose as traditional wired networks, but they allow communication between devices without the use of physical wires. Wireless technology (e.g., WiMAX [1]; IEEE 802.16 [2,3]) offers a peak downlink throughput of 46 Mbps and a peak uplink throughput of 7 Mbps. Thus, it provides almost the same downlink/uplink data rate as traditional wired networks.

With continued development of the technology, the computation capability of mobile devices has increased significantly, and they can be used to access information and services with wireless connections to the Internet. For example, business travelers can use mobile devices [4-6] to receive information from their companies or reply to e-mail. Mobile devices provide a simple way to access e-mail, and it is critical to ensure the confidentiality of e-mail. However, all data transferred via the Internet are public, so unencrypted data can be exposed to other Internet users.

The Pretty Good Privacy (PGP) [7] solution has been proposed to ensure the confidentiality and authenticity of e-mails. All content of the e-mail is encrypted and transformed into ciphertext data before being transmitted. However, if an adversary compromises the long-term private key of a user, all e-mail messages that had been sent previously might be exposed. In other words, PGP does not provide perfect forward secrecy (PFS) [8]. PFS means that the exposure of Internet users long-term private keys does not compromise previous session keys. In 2005, Sun et al. [9] proposed two secure e-mail protocols that