International Journal of Innovative Computing, Information and Control
Volume **3**, Number **2**, April **2007**

ICIC International ©2007 ISSN 1349-4198
pp. 457–469

SECURITY ANALYSIS OF SESSION INITIATION PROTOCAL

Zhaoxin Zhang
National Computer Information Content Security Key Laboratory
Harbin Institute of Technology
Harbin 150001, P. R. China
zhang_zhaoxin@pact518.hit.edu.cn

Binxing Fang, Mingzeng Hu and Hongli Zhang
Research Center of Computer Network and Information Security Technology
Harbin Institute of Technology
Harbin 150001, P. R. China
{ bxfang, zhl}@pact518.hit.edu.cn; mzhu@hit.edu.cn

Received September 2005; revised April 2006

Abstract. *With the development of multimedia technology, SIP (Session Initiation Protocol), as a simple, flexible and extensible protocol, has become the research focus of the NGN. In this case, the security issues of SIP become a very critical problem simultaneously. Through studying the security of SIP, this paper validates five attack ways in practical circumstances, including Registration Hijacking, INVITE attack, re-INVITE attack, Tearing Down Sessions, and DoS. Finally, through synthetic analysis and experiments, proposes four available measures to enhance the security of SIP: Improved Identity Authentication for HTTP Digest, Encryption with Hop-by-Hop, Forbidding the Lawless Third Part Register, Forbid the rewriting in 'From' Field and 'To' Field.*

Keywords: SIP, Attack, Encrypt, Authentication, Register

1. **Introduction.** Along with the rapid development of the information industry, multimedia communication service will become the further amalgamation of data, video and voice. In such circumstances, communication networks and data networks are combining to form the NGN (Next Generation Network), and VoIP (Voice over Internet Protocol) becomes one of the focuses in research and application. VoIP technology exists in many mature network protocols, which includes H.323 specified by ITU-T (International Telecommunication Union) and SIP (Session Initiation Protocol) [1] specified by IETF (Internet Engineering Task Force). This paper is specifically concerned with SIP, especially with the security issues.

On an IP network layered model, SIP is an application-layer signal protocol which can establish, modify or terminate multimedia session process [2] within several parts, and manage conversations, modifying the conversation parameters, assigning the services, introducing new subscribers, setting up call-transfer, call holding etc, thereby, the next generation increment service platform is composed. Now, SIP has been defined by the 3GPP (The 3rd Generation Partnership Project) as a signal protocol for the 3rd generation communication system [3]. As SIP is a text based IP telephone signal protocol, and is vulnerable to be imitated, juggled and unlawfully utilized. Signal message includes some