Proposed SecureSIP Authentication Scheme based on Elliptic Curve Cryptography

Samaneh Sadat Mousavi-Nik
MSc. of IT – Information Security
Tehran University
Tehran, Iran

M.H. Yaghmaee-Moghaddam
School of Engineering
Ferdowsi University

M.B. Ghaznavi-Ghoushchi
School of Engineering
Shahed University
Tehran, Iran

ABSTRACT
Session Initiation Protocol (SIP) is a powerful signaling protocol that increasingly used for administrating Voice over IP (VoIP) phone calls. In recent years, Session Initiation Protocol (SIP) is more and more popular. However, there are many security problems in the Session Initiation Protocol. SIP authentication mechanism is based on HTTP Digest authentication, which this scheme Is insecure; such as off-line password guessing attacks and impersonate other parties and etc. So, researches proposed different schemes to secure the SIP authentication. In the year 2012, Tang et al. proposed a SIP authentication protocol using elliptic curve cryptography (ECC), but their scheme is insecure against off-line password guessing and Registration attacks. In order to overcome such security problems proposed an ECC-based authentication scheme for SIP and analysis of security of the ECC-based protocol.
Keywords—session initiation protocol, Elliptic curve cryptography, Authentication, vulnerability, insecure

1. INTRODUCTION
Session Initiation Protocol (SIP) proposed by Internet Engineering Task Force (IETF) for the IP-based telephony [14,15].SIP controls communications on the Internet for establishing, maintaining and terminating sessions.SIP is an application –layer control protocol that is a text based protocol and can be used for controlling multimedia communication sessions such as voice and video calls over Internet protocols.[17]. SIP is the one important protocol because of the widespread application of the voice over IP (VoIP)in the Internet so the security of SIP is becoming too important[22].
SIP is a request-response protocol when a user wants to access a SIP service, at the first she/he has to authenticate with SIP server but the original authentication scheme for SIP doesn't provide enough security because it's based on HTTP Digest authentication noted in RFC2617 [8].
Different SIP authentication schemes have been proposed, especially based on Elliptic curve cryptography (ECC) to provide security for SIP. In 2005,Yang et al. found that the original SIP authentication scheme was vulnerable to off-line password guessing attack and server-spoofing attack [19] so they proposed scheme was based on Diffie-Hellman key exchange algorithm [5], which depended on the difficulty of Discrete Logarithm Problem (DLP) [10] but Yang et al.'s scheme was vulnerable to stolen-verifier attack, off-line password guessing attack, and Denning-Sacco attack [4] and Their scheme was high computation cost [6, 9, 16]. In the same year, Based on Yang et al.'s scheme, Durlanik et al. [6] introduced another SIP authentication by using Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm but this scheme in comparison with Yang et al.'s scheme reduced the execution time and memory requirements. However, their scheme still vulnerability from off-line dictionary attack and Denning-Sacco attack [12]. In 2008, Tsai [16] proposed SIP authentication scheme based on random nonce. In this scheme all the communication messages were computed with one-way hash function and exclusive-or operation so computation cost reduce highly. But this scheme vulnerable to off-line password guessing, Denning-Sacco and stolen-verifier attacks; furthermore, it did not provide any key agreement, known-key secrecy and perfect forward secrecy (PFS) [2, 3, 11, 20].In 2009, Wu et al. [23] suggested an SIP authentication scheme based on elliptic curve cryptography (ECC). This scheme achieves authentication and a shared secrecy at the same time. Wu et al.'s scheme provides provable security in the Canetti–Krawczyk (CK) security model [13] and it's suitable for applications that require low memory and rapid transactions. But Wu et al.'s SIP authentication schemes are still vulnerable to off-line password guessing attacks, Denning-Sacco attacks, and stolen-verifier attacks [10, 11]. In 2009, Yoon et al. proposed another authentication for SIP using ECC in [20]. Unfortunately, the scheme was vulnerable to password guessing attack and stolen-verifier attack. The attack method could be referred to [18]. In 2010, Yoon et al. proposed the third and fourth ECC-based authentication scheme for SIP [21, 24]. But these schemes were vulnerable to offline password guessing and stolen-verifier attacks [18]. In 2011, Arshad et al. proposed SIP authentication scheme based on ECC [2]. ButArshad et al.'s authentication scheme was vulnerable to off-line password guessing attack [1]. In 2012, Tang et al. proposed a secure and efficient authentication scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) for SIP. This paper demonstrates the Tang et al.'s authentication scheme vulnerable to off-line password guessing attack and registration attack in this paper and then propose a secure SIP authentication scheme based on ECC in order to solve those security problems. The proposed SIP authentication scheme can provide high security and executes faster than previously proposed schemes.
The remainder of this paper is outlined as follows. Section 2 reviews the original SIP authentication procedure. Section 3 introduces of Tang et al.'s scheme and discusses attack on it and in Section 4 proposed ECC-based mutual authentication scheme for SIP is presented. In section 5 discuss the security and efficiency of the proposed scheme, In Section 6, evaluate the performance of the proposed scheme. And Section 7is the conclusion.

2. SIP AUTHENTICATION PROCEDURE
The common authentication scheme for SIP is Digest Access Authentication (DAA) [8]. DAA security is based on the challenge-response pattern, and this mechanism relies on a shared secret between client and server [19] so Client pre-shares a password with the server before the authentication procedure starts. Fig. 1 shows procedure of the DAA mechanism in SIP.
(1) Client →Server: REQUEST
The client sends a REQUEST to the server.
(2) Server→Client: CHALLENGE (nonce, realm)
The server generates a CHALLENGE that includes a nonce and the client's realm. Then the server sends a CHALLENGE to the