SIP Authentication Scheme Improvement based on Elliptic Curve Cryptography

Samaneh Sadat Mousavi Nik, Mohammad Hossien Yaghmaee Moghaddam and Mohammad Bagher Ghaznavi Ghoushchi

Abstract—Session Initiation Protocol (SIP) is a powerful signaling protocol that increasingly used for administrating Voice over IP (VoIP) phone calls and in current Internet protocols such as Hyper Text Transport Protocol (HTTP) and Simple Mail Transport Protocol (SMTP). SIP controls communications on the Internet for establishing, maintaining and terminating sessions. But The authentication mechanism proposed in SIP specification is based on HTTP Digest authentication which this scheme has security problems, such as off-line password guessing attacks and impersonate other parties or charge calls to others and etc. So, many 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, registration and modification attacks. In this paper we try to propose an ECC-based authentication scheme for SIP to overcome such security problems. At the end, analysis of security of the ECC-based protocol shows that our scheme is suitable for the applications with higher security requirement.

Index Terms—SIP protocol, Elliptic curve cryptography, Authentication, vulnerability, security

1. INTRODUCTION

IN today's and future wired or wireless networks, multimedia service is a great importance application class. Especially, the next generation of wireless networks will be based on all-IP architecture. One of the most important protocols supporting multimedia services is the session initiation protocol (SIP)[5]. Session Initiation Protocol is an open signaling protocol standard developed by the Internet Engineering Task Force (IETF) in cooperation with many industry leaders, including Avaya, for establishing, managing, and terminating real-time communications over large IP-based networks, such as the Internet.

In 1999, SIP proposed by Internet Engineering Task Force (IETF) for the IP-based telephony [2, 3]. 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 such as Hyper Text Transport Protocol (HTTP) and Simple Mail Transport Protocol (SMTP)[4] . 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[5].

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 [6].

Different SIP authentication schemes have been proposed especially based on Elliptic curve cryptography (ECC) to provide security for SIP. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers [7].In this paper, we investigate SIP Authentication Scheme based on Elliptic Curve Cryptography, Currently, the security of SIP is becoming more and more important. SIP specification does not include any specific security mechanisms. SIP authentication is inherited from HTTP Digest authentication, which is a challenge-response based authentication protocol [2].

2. HISTORY AND RELATED WORK

In 2005,Yang et al. found that the original SIP authentication scheme was vulnerable to off-line password guessing attack and server-spoofing attack [8]so they proposed scheme was based on Diffie-Hellman key exchange algorithm [9],which depended on the difficulty of

- *S.S Mousavi Nik MSC in department of Engineering , Security in Information Technology, University of Tehran Kish International Campus, Niayesh Blvd., Kish Island, Iran*
- *M.H. Yaghmaee-Moghaddam School of Engineering Ferdowsi University Mashhad, Iran*
- *M.B. Ghaznavi-Ghoushchi School of Engineering Shahed University Tehran, Iran*