Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Obscuring users' identity in VoIP/IMS environments

Nikos Vrakas[a,*], Dimitris Geneiatakis[b], Costas Lambrinoudakis[a]

[a] Department of Digital Systems, University of Piraeus, 18532 Piraeus, Greece
[b] Digital Citizen Security Unit, Joint Research Center, European Commission, Greece

ARTICLE INFO

Article history:
Received 20 August 2013
Received in revised form
30 January 2014
Accepted 1 April 2014

Keywords:
Anonymity
Identity protection
IMS
Privacy
SIP
VoIP

ABSTRACT

Next Generation Networks bring together wired and wireless architectures, under the umbrella of an all IP architecture. Architectures such as the IP Multimedia Subsystem (IMS) offer advanced services at very low cost but also inherit IP infrastructure's security and privacy issues. The utilized signalling protocol (i.e. Session Initiation Protocol) and the related specifications are both overlooking users' privacy, leaving public and private identities unprotected to eavesdroppers. Existing solutions require either the existence of a public key infrastructure or the establishment of the appropriate mechanism for managing symmetric keys.

We propose a novel one-time identity mechanism for obscuring users' real identity against eavesdroppers. The solution exploits the advantages of commutative functions, enabling the communicating parties to exchange data without pre-established keys nor any modification in the infrastructure. All participating entities generate one-time random identities providing in this way unlinkability and anonymity services as well.

We evaluate the proposed mechanism through an open source IMS platform. Results have provided evidence that the client's response times are not considerably affected by the proposed mechanism, while the overhead imposed to the IMS core is negligible.

Introduction

The IP Multimedia Subsystem (3GPP, 2011) enables mobile and landline infrastructures to access multimedia and Internet services through an all-IP architecture. Users can access and share multimedia services independent of the device type, at very low cost. The architectures employ the Session Initiation Protocol (SIP) (Rosenberg et al., 2002) for session management. SIP is a lightweight and easily extendable protocol comprised of clear text messages, loose syntactic rules and flexibility in incorporating new services into the architecture.

However, many researches have highlighted a series of security and privacy issues (Geneiatakis et al., 2006; Park and Park, 2007; Bremler-Barr et al., 2006; Vrakas et al., 2011, 2010; Keromytis, 2011) of SIP-based applications for IP and mobile networks. This is mainly because sensitive information (e.g. user identity) traverses the network, during session management, unprotected. An eavesdropper can capture such information and associate it with actions, services and calls, compromising users' privacy and anonymity. For instance, a

[*] *Corresponding author*. Tel.: +30 6948043744.
E-mail addresses: nvra@unipi.gr (N. Vrakas), dimitrios.geneiatakis@jrc.ec.europa.eu (D. Geneiatakis), clam@unipi.gr (C. Lambrinoudakis).

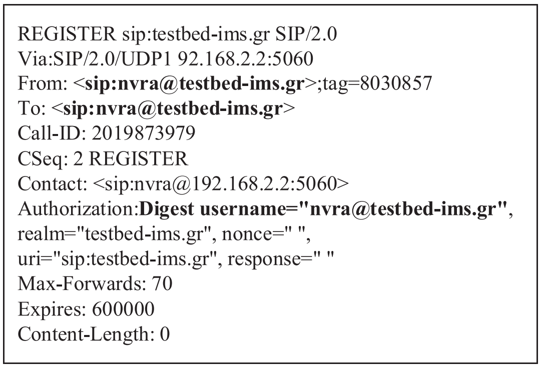
http://dx.doi.org/10.1016/j.cose.2014.04.001
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

malicious user who is monitoring the signalling messages exchanged, can easily profile users' preferences and associate users' identities with other accounts in order to launch unsolicited advertises such Spam over Internet Telephony (SPIT) (Biever, 2004), or denial of service attacks against legitimate users.

The SIP specifications (Rosenberg et al., 2002) do not provide a mechanism that can adequately preserve users' privacy. An extension mechanism that enhances users' privacy has been proposed in (Peterson, 2002; Jennings and Peterson, 2002), but even in that mechanism the user identity remains unprotected during the first hop (between the user and the proxy server) and it is mainly focused on concealing private information from the callee or when the singling terminates outside of the domain. Moreover, it does not provide any protection to the identity of the call receiver (namely the callee) and thus an eavesdropper can determine the person that the initiator intents to call. In addition the latter scheme is vulnerable to security degrading attacks. Coming to IMS, its security specifications (3GPP, 2010) do not either propose any countermeasures for user identity protection. One might assume that the employment of a mechanism such as S/MIME (Ramsdell, 1999) could facilitate the protection of signalling's sensitive information but, on the other hand, the digital certificates involved may disclose user's identity. Alternatively, the Authentication and Key Agreement (AKA) with IPSec and the SIP Digest with TLS (3GPP, 2010) can protect users' privacy since they provide confidentiality and integrity services to the communication. However, during the registration procedure, the user must provide his identity in clear text. On top of that, the aforementioned security protocols are not supported by devices with limited resources.

The contribution of other research work in this field (Ramsdell, 1999; Karopoulos et al., 2008, 2010; Castleman) is considered limited. The proposed schemes either require modification in the underlying infrastructure or the deployment of additional network entities (Castleman). The employment of a Public Key Infrastructure (PKI) is proposed in (Ramsdell, 1999; Karopoulos et al., 2010) which involves among others digital certificate management, signing, revoking and updating procedures. On the other hand, symmetric encryption techniques introduce key related concerns (e.g. key exchange/agreement protocols, key storing).

To the best of our knowledge, our proposal is the first work that protects users' identities in VoIP and NGNs without: (a) modifying the underlying infrastructure, (b) requiring a key management scheme, (c) an additional key exchange scheme (d) a PKI infrastructure and finally (e) without a prior-knowledge between the communicating entities as the other schemes require. Moreover, it provides protection from the first hop of the communication and thus the identity remains concealed even in untrusted and trusted domains. Finally, it can conceal both members of the communication (caller and callee) identities when requested. The proposed mechanism is based on Shamir's keyless scheme (Shamir, 1980) and utilizes the commutative functions in order to obscure and conceal users' real identities included in SIP signalling messages. The commutativity property enables the communicating parties to exchange data without a key or prior knowledge. The protocol uses the commutativity of the modular exponentiation and its computational complexity is equivalent to the discrete logarithm problem (DLP) (McCurley, 1990). The experimental results show a negligible amount of delay in scheme's calculations both for client and server sides.



```
REGISTER sip:testbed-ims.gr SIP/2.0
Via:SIP/2.0/UDP1 92.168.2.2:5060
From: <sip:nvra@testbed-ims.gr>;tag=8030857
To: <sip:nvra@testbed-ims.gr>
Call-ID: 2019873979
CSeq: 2 REGISTER
Contact: <sip:nvra@192.168.2.2:5060>
Authorization:Digest username="nvra@testbed-ims.gr",
realm="testbed-ims.gr", nonce=" ",
uri="sip:testbed-ims.gr", response=" "
Max-Forwards: 70
Expires: 600000
Content-Length: 0
```

Fig. 1 – A SIP REGISTER request. The private and public users' identities (in bold) are unprotected and can be captured by passive eavesdroppers.

The rest of the paper is structured as follows: Issues concerning privacy in SIP-based architectures are presented in Section Privacy issues. A detailed description of the proposed mechanism is provided in Section Proposed protection. The experimental results are presented in Section Evaluation, while a comprehensive literature review can be found in Section Related work. The paper concludes with directions for future work in Section Conclusions and future work.

Privacy issues in IP Multimedia Subsystem architecture

In IMS the signalling protocol utilized for the management of multimedia sessions is SIP (Rosenberg et al., 2002). The protocol's key features include: (i) flexibility, which provides the developers with the opportunity to easily incorporate and implement new capabilities and services and (ii) text-based structure, a feature that renders it a lightweight protocol suitable for time sensitive services. An example of a SIP

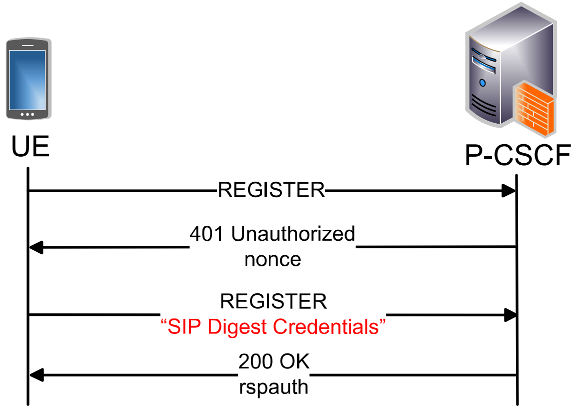


Fig. 2 – SIP registration/authentication handshake with the SIP digest authentication protocol.