APPLYING SRP ON SIP AUTHENTICATION

Celalettin Kilinc and A. Gokhan Yavuz
Computer Engineering Department, Yıldız Technical University, Beşiktaş, İstanbul, Turkey

Keywords: Sip security, authentication, key exchange, secure remote password.

Abstract: Session Initiation Protocol (SIP) is the leading protocol used in IP telephony today. By the increasing use of IP telephony and also SIP, features like QoS and security are becoming more and more important. Because of the its simple design, SIP does not have a highly secure authentication mechanism which needs to be enhanced in order to cope with today's security threats of IP. In this paper we propose a new authentication scheme for SIP based on the Secure Remote Password (SRP) Protocol. Our proposed authentication scheme modifies two existing SIP messages and adds a new SIP message. The result is a verifier based authentication scheme for SIP in which client passwords do not need to be sent to the registrar service in any form.

1 INTRODUCTION

Internet telephony offers more features and services then the POTS and because of this, it has wider application areas. In classical telephony services circuit switching is used between communicating parties, which assures both a certain level of quality of service and security. On the other hand, IP telephony is based on packet switching and uses the public Internet for communication, thus it faces all the quality of service problems and security threats of the Internet.

SIP (Rosenberg, 2002) is the leading protocol for IP telephony. It has a simple yet efficent design which mainly provides for performance. Because of its simplicity, SIP does not have a complete security mechanism. Therefore, SIP's security features must be enhanced especially for the authentication of the communicating parties.

There are some studies on security mechanisms of SIP. (Qi, 2003) proposed an additional authentication procedure between proxy and user agent server beside the authentication between user agent client and proxy. In another study (Srinivasan, 2005), when clients make requests to the proxy server, proxy server assures the identity of the clients from the registrar server. (Durlanik, 2005) proposed a new approach for secure SIP authentication by using a public key exchange mechanism using Elliptic Curve Cryptography. (Holger, 2007) studied on a refinement in security for call centers. In his security scheme proxy servers add a signature to SIP messages that come from known users.

In this paper we present a new SRP based authentication mechanism for SIP. While this new authentication mechanism works without sending client passwords neither plaintext nor hashed, it requires only minor modifications to the original SIP protocol and has no noticable impact on the performance of SIP.

The outline of our paper is as follows. In section 2 we give a brief overview of current SIP authenticaion mechanisms, in section 3 we discuss the most common security threats against SIP and in section 4 we look at alternative authentication mechanisms which can be applied to the SIP. Section 5 is where we propose our new authentication scheme for SIP. In section 6, we conclude our paper.

2 SIP AUTHENTICATION

Authentication is certainly needed at several points of SIP communication. For example, during the registration process, the registrar must ensure that it registers the authorized SIP endpoint and it must protect the system from malicious user registrations. Furthermore if a SIP endpoint wants to setup a session using an INVITE message, it needs to know that it is communicating with the right endpoint. Authentication is also mandatory when a party wants

Kilinc C. and Gokhan Yavuz A. (2008).
APPLYING SRP ON SIP AUTHENTICATION.
In *Proceedings of the International Conference on Security and Cryptography*, pages 227-231
DOI: 10.5220/0001929702270231

to modify the session parameters. Unauthorized parties must not be allowed to change the parameters of a session. Also in the case of terminating a session, only the authenticated parties must be allowed to do so by sending a terminate a *BYE* message.

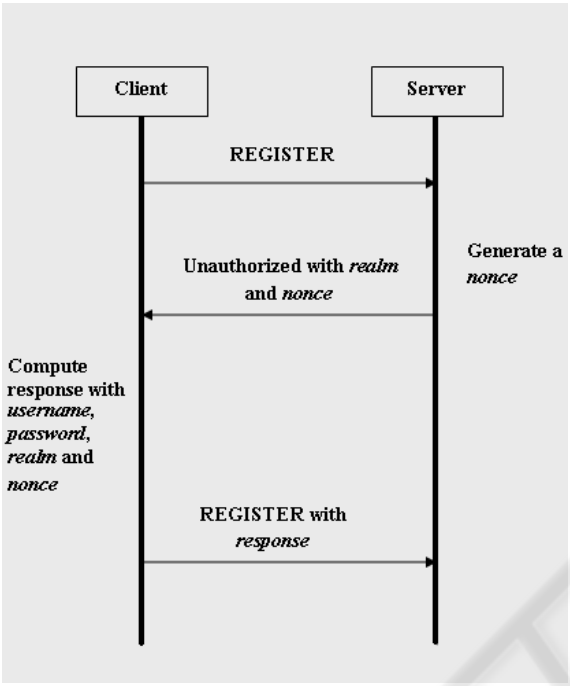

Figure 1: SIP authentication steps with challenge-response.

SIP is an application level protocol and inherits its authentication mechanism from HTTP and provides a challenge-based mechanism for authentication (Franks J, 1999). This type of authentication is also known as digest authentication. We will show the challenge-response authentication in SIP by a SIP registration process example.

When a SIP client wants to register itself, it sends a *REGISTER* message to the registrar server, as depicted in Figure 1. The registrar server replies to the client with an *Unauthorized* message containing a nonce value. The nonce value is a randomly generated unique value which is sent with every challenge message. Clients must respond to the challenge messages by using the corresponding nonce value. When the client gets the *Unauthorized* message, it computes a hash value (3) based on its identity, password and the nonce value. This hash value will be sent in the new *REGISTER* message to the registrar server. The *realm* value in (1) is used to specify the domain where the authentication takes place. The *digestURI* is the uniform resource identifier used in SIP protocol.

$$HA1=MD5(username:realm:password) \quad (1)$$

$$HA2= MD5(method:digestURI) \quad (2)$$

$$response= MD5(HA1:nonce:HA2) \quad (3)$$

The default hash algorithm used in SIP authentication is MD5, but it can be changed by setting the algorithm property of the SIP message. When the registrar receives the new *REGISTER* message with response value, it computes the same value with clients password, identity and nonce, to decide going on registering or denying the client.

3 SIP SECURITY THREATS

SIP is based on IP and therefore it can be the victim of various IP based attacks. These attacks are grouped according how they are applied and their details are given in the following subsections.

3.1 Replay Attack

Replay attacks can be dangerous for protocols that use messages in their communication such as SMTP, HTTP, SIP and etc. An eavesdropper can obtain the session parameters of a SIP communication by listening and recording the entire SIP messaging between the communicating parties and thus he can perform a replay attack afterwards. In this attack, he can imitate real SIP parties by replaying recorded messages to other SIP parties in order to establish forged session with them. The standard SIP authentication procedure tries to protect itself from simple replay attacks by the use of the nonce values in the challenge messages. With the nonce values, response to each *REGISTER* message will have a unique identification which makes replay attacks harder.

3.2 Chosen Plaintext Attack

SIP secrets can be attacked by chosen plaintext attacks. Parameters of a successful authentication session can be listened and obtained by the attacker. Once the attacker handled the username, realm and the nonce parameters in (1), (2) and (3), he can try to find the password by giving predicted values for the password.

3.3 Registration Hijacking

In SIP, participants register themselves to registrar servers, therefore malicious registrations are one of the security threats that SIP faces. An attacker can try to register himself to registrar server as a legitimate user of the system and thus he can receive all the calls originating for this user whose registration he has hijacked. SIP uses UDP for messaging and as UDP is a connectionless transport protocol, either outstanding UDP messages can be modified or new UDP messages can be injected very easily. Therefore, forged SIP messages can be built and sent for the purposes of registration hijacking. As given in section 2, SIP uses a challenge-response authentication mechanism and therefore a hashed version of the user's password is sent via the network during the registration process. Once the password is captured by an attacker this password can be cracked with an offline dictionary attack. Using the cracked password the attacker can easily register himself to the registrar server as the victim. To overcome this vulnerability SIP authentication procedure must be strengthened such that the passwords will not be sent during the registration process.

Our proposed authentication mechanism overcomes this vulnerability by sending the password in neither plaintext nor hashed version.

4 AUTHENTICATION MECHANISMS

Authentication systems can be divided into two types: plaintext equivalent based systems and verifier based systems (Wu, 1998). Plaintext equivalent based systems require the authentication server to store a copy of the user passwords. If a user wants to be authenticated, he sends his password to the authenticator either plaintext or hashed. The authenticator checks the received password against the one in its database. Verifier based authentication systems, on the other hand, require only a verifier to be stored in their database and passwords are not used in communication in any form.

Verifier based systems have great advantages over the plaintext equivalent based ones. In plaintext equivalent based systems, for malicious third parties there exists always the possibility to obtain a copy of the password (plaintext or hashed) either by eavesdropping the communication or by accessing the password database. A secure authentication system is expected to leak the minimum possible amount of data regarding the authentication process. Therefore, verifier based systems reduce the risk of exposing critical information about the authentication process.

In the following subsections first we will give brief information on challenge-response based authentication as an example of plaintext equivalent based systems. Then after touching the fringes of Encrypted Key Exchange, we will give some basics on Asymmetric Key Exchange and go onto the construction of Secure Remote Password from AKE.

4.1 Challenge-Response

Plaintext equivalent based systems use secrets or hashed equivalents in communication. For this reason they can be vulnerable in networks that have a risk to be eavesdropped. To decrease this risk and repair this vulnerability, a challenge based mechanism is suggested (Franks, 1999). When a service request is received by the authenticator party, a challenge message is sent to the requesting party with a random and unique qualifier. The requesting party computes a response containing its identity, password and the unique value received. It then replies to the challenge request with this response. The authenticating party computes the same response as well and by comparing the computed response with the received response, it decides the success of the authentication attempt. This mechanism provides some refection on plaintext equivalent systems. This is provided by the random value that is unique for every session. By using this unique value, each response that is calculated and sent over network will be different and a captured response value will not mean that password is captured. This mechanism also prevents the system from a simple replay attack. However challenge based systems can be attacked by using captured response values and the randomly generated challenge unique values of successful authentications as the input to an offline dictionary attack. In cases where SIP agent passwords are chosen simple, which is almost always the case in practice, passwords can be cracked very easily.

4.2 Encrypted Key Exchange

Encrypted Key Exchange (EKE) is an example of verifier based authentication systems (Bellovin and Merritt 1994). EKE basically uses Diffie and Hellman's (1976) general key distribution system and extends it by encrypting the all data with a private key in all communication. This prevents any

other listening party to have information about the authentication procedure. After EKE, some other extending protocols are developed based on EKE. DH-EKE (Steiner, Tsudik and Waidner, 1995) and SPEKE (Jablon 1996) are two of these. These protocols aim not to give useful information to the attacker to obtain secrets and keys of the sessions.

EKE has become a strict and reliable solution for password based authentication systems. However EKE still has a vulnerability. Like other plaintext-equivalent ones, user or host accesses to a shared password or a hashed version of it. To overcome this weakness another version of EKE, Augmented EKE was developed (Bellovin and Merritt, 1994), which makes EKE a verifier–based protocol. (Wu, 1998) says this modification destroys forward secrecy, which means data that an attacker captured is not useful for future sessions.

4.3 Asymmetric Key Exchange and Secure Remote Password

Asymmetric Key Exchange (AKE) uses key exchanging between user and host to verify that the two parties know the same secret as in EKE. But, AKE does not use encryption in communication. It uses predefined mathematical relationships for verifying passwords with exchanged values. “Avoiding encryption is advantageous for a number of reasons” says (Wu, 1998) and explains them as reasons of not using encryption while defining SRP protocol.

As (Wu, 1998) described, AKE is a set of mathematical relations and guaranties nothing about the security of the resulting protocol. It depends on the chosen functions for the equations that AKE specifies. We can say that AKE is a structure and skeleton of an authentication protocol. Implementations and applications of AKE will be new protocols based on AKE. (Wu, 1998) describes Secure Remote Password (SRP) by filling in the functions in AKE’s skeleton. Mathematical relations and working of SRP is described in detail in (Wu, 1998). We will use SRP in our proposed scheme for SIP authentication.

5 APPLYING SRP ON SIP AUTHENTICATION

SIP authentication procedure must be enhanced and its security must be expanded because of the reasons we argued in the previous sections of this paper. A closer look at the Secure Remote Password Protocol (Wu, 1998) itself and its working steps reveals that SRP can be applied as the authentication procedure for SIP communication. First we will give some detail on the negotiation steps of SRP and then explain how they can be used for SIP authentication.

In Figure 2 SRP negotiation steps are given using a simple pseudo code notation to explain the transactions between a client and server. A SRP negotiation is initiated by the client by sending its username to the server. Then the server responds with a reply message which includes the *modulus*, *generator* and *salt* parameters. The usage of these parameters is explained in (Wu, 1998). The client generates and sends its public key based on the received parameters and expects to receive the servers’ public key. Upon successful reception of public keys, both the client and the server compute the session key, and the client sends a response, encrypted with the computed session key, to the server to authenticate itself. The server verifies the received response and sends back a positive or negative acknowledgement depending on the authentication status.

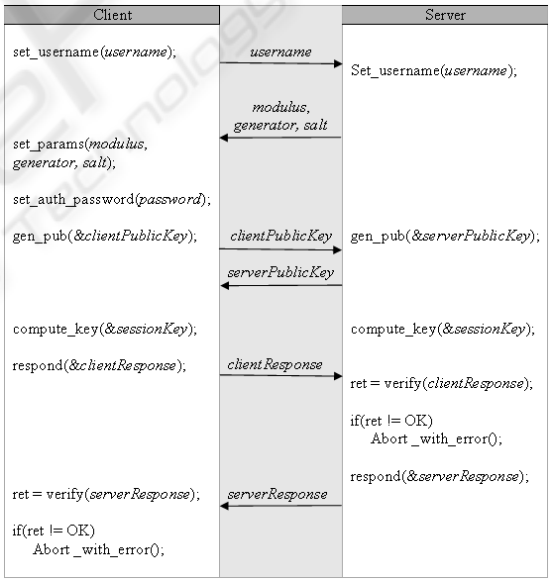

Figure 2: SRP negotiation steps.

It is very obvious that the negotiation steps of SRP and the authentication steps of SIP follow a very similar scheme. In SIP authentication a client which received the *Unauthorized* message from the server in response to its initial *REGISTER* message, calculates a response value and sends that value in the new *REGISTER* message in an attempt to authenticate itself to the registrar server. This calculated response value in the new REGISTER

message is where we will be applying SRP for authentication in SIP.

In our proposed new authentication scheme, a SIP client will send its username in the initial *REGISTER* message. Instead of replying with standard SIP parameters in the *Unauthorized* message, our implementation replaces those parameters with SRP parameters. When the client receives the *Unauthorized* message with the SRP parameters it computes its public key as in SRP. At the same time the registrar server also computes its public key for an exchange with the client. As there is no step for exchanging keys in the SIP authentication, we have defined an extra SIP message for the exchange of client and server public keys. When both parties have the other's public key they compute the session key, and the client generates a response value encrypted using the computed session key and sends it to the registrar server in the new *REGISTER* message. Thus there is no need to define a new SIP message for this step. When the new *REGISTER* message arrives at the registrar server, it verifies the authenticity of the client using the response value contained in the message. The flow of our SRP based new SIP authentication scheme is given in Figure 3.

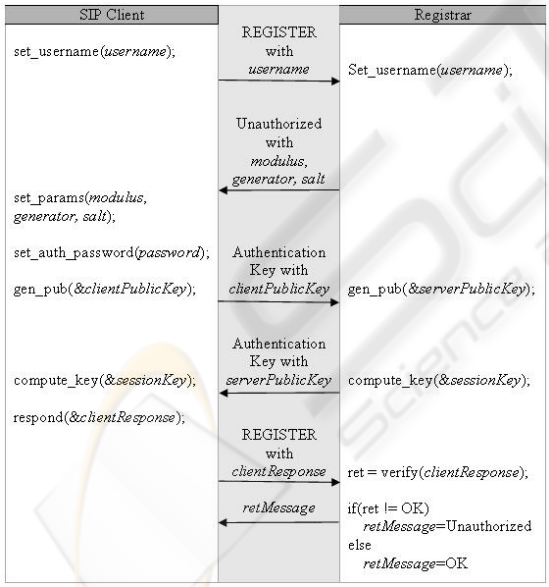

Figure 3: SIP authentication with SRP.

6 CONCLUSIONS

SIP has a wide and increasing area of applications and SIP security is one of the most important details which must not be overlooked. Because of its simple design initial implementations of SIP protocol did not give the first priority to the security, but today it is inarguable that security is of utmost concern for any IP based application. So, by adding only a new SIP message and replacing the parameters in two existing SIP messages we have demonstrated that SRP can be used for SIP authentication without having the client password to be sent in any form over the underlying communication network.

For future work we will modify the SIP authentication mechanism to provide for server authenticity as well.

REFERENCES

Bellovin, S.M. and Merritt, M., Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. Technical report, AT&T Bell Laboratories, 1994.

Diffie W., Hellman M.E., New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644{654, November 1976.

Franks J., Hallam-Baker P., Hostetler J., Lawrence S., Leach P., Luotonen A., Stewart L., HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, June 1999

Jablon D. Strong password-only authenticated key exchange. Computer Communication Review, 26(5):5{26, October 1996.

Steiner M., Tsudik G., and Waidner M., Refinement and extension of encrypted key exchange. ACM Operating Systems Review, 29(3), July 1995.

Wu T., "The Secure Remote Password Protocol", March 1998

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Qi, Q., Study of Digest Authentication for Session Initiation Protocol, SITE, University of Ottowa, (2003)

Srinivasan R., Vaidehi V., Harish K., LakshmiNarasimhan K., LokeshwerBabu S., Srikanth V. (2005) "Authentication of Signalling in VoIP Applications", 2005 Asia-Pacific Conference on Communications, 3 - 5 October 2005, Perth, Western Australia.

Holger S., Chi-Tai D., Franz J. H., "Proxy-based Security for the Session Initiation Protocol (SIP)", Second International Conference on Systems and Networks Communications, IEEE, 2007

Durlanik A., Sogukpinar I., SIP Authentication Scheme using *Ecdh, Proceedings Of World Academy Of Science, Engineering And Technology*, Volume 8, October 2005 ISSN 1307-6884