一种基于改进的 HTTP 摘要认证的 SIP 安全机制*

彭焕峰

(南京工程学院 计算机工程学院,江苏 南京 211167)

摘 要:SIP 协议是当前 IP 电话中的主流协议,HTTP 摘要认证机制被很多 SIP 系统作为安全机制,但存在客户端不能认证服务器端,且不支持密钥协商的缺陷。为解决这一不足,提出了一种基于改进的 HTTP 摘要认证的 SIP 安全机制,使得 SIP 安全解决方案更加完善,部署更加灵活。

关键词:SIP;HTTP 摘要认证;安全机制

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2011)06-0053-03

SIP security mechanism based on improved HTTP digest authentication

Peng Huanfeng

(School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: SIP is the shortening of session initialization protocol. Many SIP systems use HTTP digest authentication mechanism as their security mechanism, but the client can not authenticate the server, and key agreement is not supported. This paper gives one security mechanism of SIP based on an improved HTTP digest authentication, this security mechanism resolves the defects above, and makes the security solution more perfect and flexible.

Key words: SIP; HTTP digest authentication; security mechanism

SIP 协议即会话发起协议[1],是 NGN 网络和 3G 网络的核心协议,目前在电信网络中有着广泛的应用。由于 SIP 协议的消息以文本方式编码,容易阅读解析,并且 SIP 消息在开放式的 IP 网络中传输,SIP 消息容易被攻击者模仿、篡改,然后加以非法利用,最终导致账号被盗用、业务失败或被干扰。目前很多 SIP 系统采用基于 HTTP 摘要认证机制作为系统的安全解决方案[2-3],但该机制有两个主要的缺陷,即不能满足客户端认证服务器端,也不具有密钥协商机制。为能够对 SIP 消息中的头域进行端到端的加密,本文提出了一种改进的 HTTP 摘要认证机制,解决了基于 HTTP 摘要认证的 SIP 安全机制的缺陷。

1 基于 HTTP 摘要认证的 SIP 安全机制

HTTP 摘要认证机制解决了基本认证机制密码明文传输的问题,但同样基于用户名密码体系,并没有建立初始用户名密码体系的机制[4],SIP 系统可以基于 HTTP 摘要认证建立自己的安全机制。

1.1 认证流程

在基于 HTTP 摘要认证的 SIP 安全机制中,摘要认证的架构与 HTTP 摘要认证的架构非常相似,特别是认证模式、认证参数、挑战、域、域值和凭证的 BNF 都是一样的。两者都是基于挑战-响应模式。如果客户端(UAC)发起的请求没有包含认证信息,则服务器(UAS 或者 Proxy)会向客户端发起挑战,挑战信息包含在 401/407 响应中,客户端收到挑战后,用 ACK 请求确认挑战,然后重新构建包含认证信息的请求,服务器认证成功后,则接受此请求。SIP 认证对特定域有意义,每个保护域都有自己的用户名和密码,服务器在其挑战中应该包含域信息,提示客户端提供此域的用户名和密码信息。

1.2 存在的缺陷

摘要认证是基于预分配用户名密码的一种认证机制,主要目的是替代基本认证,避免密码在网络中明文传输。摘要认证机制可以解决注册劫持、请求欺骗、重放攻击、篡改消息等安全问题,同时还能提供一定的完整性保护[5]。

摘要认证的缺陷主要有:(1)没有提出完备的双方认证机制,即 UAC 不能对 PROXY 和 UAS 进行认证,容易遭受伪装服务器攻击;(2)没有密钥协商机制,不能协商私密密

* 基金项目:南京工程学院科研青年基金项目(QKJB2009026)

钥,然后对 SIP 指定头域进行加密,避免信息泄漏。

2 基于改进的 HTTP 摘要认证的 SIP 安全机制

针对摘要认证机制的两点主要缺陷,经过对摘要认证机制的深入研究和实践总结,论文提出了一种基于改进的 HTTP 摘要认证的 SIP 安全机制。

2.1 改进后的认证流程

呼叫建立的效率与信令的数量有关,在 SIP 协议上应用认证方案时,不能过多地引入信令流程,从而较大程度地影响呼叫效率。因此改进的认证方案充分利用原有的认证信令流程,扩充了 4 个 SIP 头域:UAC-Authenticate、UAC-Authorization、Encryption-Info、Encrypted-Header,实现了客户端与服务器的双向认证和加密密钥协商机制,而无需扩充新的信令流程。以 INVITE 请求为例,改进后的认证流程如图 1 所示。

图 1 改进后的摘要认证机制认证流程

由图 1 可以看出,改进的摘要认证机制并没有更改原有的信令流程,而是通过扩充 SIP 头域来解决摘要认证机制存在的主要缺陷。

UAC 认证 UAS/PROXY 的流程为:

(1)UAC 向服务器发起请求,若需要认证服务器,则在请求的 UAC-Authenticate 头域中包含挑战参数,向服务器发起挑战;

(2)服务器在收到含有挑战信息的请求后,如果是针对自己的挑战,则获取 UAC 的帐号密码,连同挑战参数,生成凭证,并在 401/407 响应的 UAC-Authorization 头域中包含此凭证;

(3)UAC 在收到 401/407 响应后,验证响应中包含的凭证,如果有效则证明服务器知道自己的用户名和密码,可以进行后续处理。

密钥协商流程为:

(1)服务器收到客户端的请求后,若配置了密钥协商策略,则在 401/407 响应的 Encryption-Info 头域中提供自己的公钥加密算法、公钥、支持的对称加密算法等信息;

(2)UAC 收到包含 Encryption-Info 头域的 401/407 响应时,根据自己的安全策略,若支持改进的摘要认证机制,则通过 ACK 请求返回自己的对称加密密钥(用服务器提供的公钥加密)和选择的加密算法;

(3)在上述两步中双方建立了加密上下文,UAC 在再次发起的请求中可以对某些头域进行加密。

值得说明的是,一般 SIP 系统中服务器作为操作的主导,因此改进的认证机制在加密协商时,只能由服务器主动发起协商,同时为了能够协商加密密钥,服务器需要有公钥加密机制。

2.2 客户端和服务器端操作规范

类似 IETF 的 RFC3261[1]文档,对于改进的摘要认证机制需要给出客户端和服务器端的操作规范,在此以 INVITE 请求为例,对客户端和服务器端的操作规范进行描述。

客户端操作规范:

(1)根据安全策略配置,如果需要对服务器端进行认证,则在发送的 INVITE 消息中携带 UAC-Authenticate 头域,包含要认证的服务器端的 URL(包含在 digest-uri 参数中)、username、qop、nonce 等参数。

(2)在接收到服务器端返回的 401/407(UAS 返回 401,Proxy 返回 407)响应后:

①如果响应包含 UAC-Authorization 头域,则计算凭证,如果与服务器端返回的凭证相同,则表明服务器端知道 UAC 的密码,这样就完成了对服务器端的认证。如果验证不通过,则发送 ACK 对 401/407 响应进行确认后,UAC 不再发起新的请求;

②如果响应包含 WWW-Authenticate/Proxy-Authenticate 头域,则表明服务器端要求认证 UAC,缓存挑战参数以在重新发起的请求中计算凭证;

③如果响应包含 Encryption-Info 头域,则表明服务器端发起加密协商请求,该头域中包含服务器端的公钥及其支持的加密算法等信息。

(3)UAC 对 401/407 响应发送 ACK 进行确认,如果 401/407 响应中包含 Encryption-Info 头域,且 UAC 也配置为支持加密协商,则 ACK 请求中应包含 Encryption-Info 头域,告知 UAC 随机生成的加密私钥(经过服务器端的公钥加密)和采用的加密算法。

(4)UAC 重新发起请求,如果服务器端要求认证 UAC,则在新的请求中包含 Authorization 或者 Proxy-Authorization 头域,向服务器提供凭证。如果之前成功地进行了密钥协商,则对需要加密的头域可以用私密密钥进行加密。

服务器端操作规范:

(1)若客户端需要验证服务器端,则服务器端在收到的第一个 INVITE 请求中包含 UAC-Authenticate 头域,提供 digest-uri、username、nonce、qop 等挑战参数;

(2)根据认证策略的配置,服务器端在收到请求时做如下处理:

①如果请求包含 UAC-Authenticate 头域，且头域中的 digest-uri 参数的指示是自身，表明 UAC 要认证自己，所以要计算凭证，返回 401/407 响应(凭证包含在 UAC-Authorization 头域中)；

②如果请求中没有包含 UAC-Authenticate 头域，则表明 UAC 并不想认证自己，如果服务器端不需要认证 UAC，继续处理 INVITE 请求；

③如果服务器端需要认证 UAC，则返回 401/407 响应，并在响应中包含 WWW-Authenticate/Proxy-Authenticate 头域，提供挑战信息；

④如果服务器端配置了加密协商策略，则在收到 UAC 的请求后，返回 401/407 响应，在 Encryption-Info 头域中包含自己的公钥加密算法、公钥和支持的加密算法，向 UAC 提起加密协商挑战。

若客户端与服务器端要求相互认证，且服务器端配置了加密协商策略，则在对客户端请求的 401/407 响应中就会同时包含 UAC-Authorization、Encryption-Info、WWW-Authenticate/Proxy-Authenticate 头域。

(3)接收到 UAC 对 401/407 响应的 ACK 确认消息后：

①如果 ACK 消息中包含 Encryption-Info 头域，则表明 UAC 支持加密协商，其中 Encryption-Info 头域中包含 UAC 给定的加密私钥(用服务器端的公钥加密)、加密算法等信息。服务器端应该缓存 Encryption-Info 头域的内容，以用来处理后续的请求；

②如果 ACK 消息中没有包含 Encryption-Info 头域，则表明 UAC 不支持加密协商。

(4)经过密钥协商后，则后续消息的部分头域在整个会话期间可能做了加密处理，服务器端应该先对加密的头域进行解密，然后验证 UAC 提供的凭证。

2.3 扩展头域规范

改进的摘要认证机制对 SIP 协议进行了扩展，新增 UAC-Authenticate、UAC-Authorization、Encryption-Info、Encrypted-Header 四个头域。

其中 UAC-Authenticate 头域的规范类似于 WWW-Authenticate，而 UAC-Authorization 头域规范类似于 WWW-Authorization，仅有部分区别。

Encryption-Info 头域携带了密钥协商信息，服务器在 401/407 响应中用此头域告知客户端服务器侧使用的公钥加密算法、加密公钥，支持的对称加密算法；客户端在对 401/407 响应的 ACK 请求中用此头域告知服务器使用的对称加密的私钥以及选择的加密算法。该头域规范如下：

Encryption-Info="Encryption-Info"":" Encrypt-Info

Encrypt-Info=1#(public-key| public-encrypt-algorithm| encrypt-private-key | algorithm | [encrypt-param])

public-key="public-key " "= " key-value

key-value?= quoted-string

public-encrypt-algorithm=" public-encrypt-algorithm " "=" key-value encrypt-private-key="encrypt-private-key " "=" key-value

algorithm="algorithm" "=" <"> 1# algorithm-value <">

algorithm-value="DES" | "DEA" | token

public-key 参数由服务器端指定，告知客户端自己的公钥。

public-encrypt-algorithm 参数由服务器给出，指定了服务器使用的公钥加密算法。

encrypt-private-key 参数给出客户端指定的对称加密私钥，用 public-key 参数中指定的公钥加密后传给服务器端。

algorithm 参数列出了服务器端支持的对称加密算法；客户端发送至服务器端的 ACK 消息中此参数应为客户端选定的加密算法，且此算法应包含在服务器端支持的加密算法列表中。

Encrypted-Header 头域表示加密后的头域，其 BNF 范式如下：

Encrypted-Header="Encrypted-Header"":" Encrypt-Value

Encrypt-Value=quoted-string

例如对头域 From:B <SIP:B@Nanjing.com> 进行加密，假设加密后该头域成为：Encrypted-Header: 8f831abf39815iodhe83d20acA2B，当对端收到有加密头域的 SIP 消息时，首先对 Encrypted-Header 头域进行解密处理，还原出原有头域，然后进行后续处理。

针对基于 HTTP 摘要认证的 SIP 安全机制不能实现客户端主动认证服务器端、可能受到伪装服务器的安全威胁，同时不能在客户端和服务器端进行密钥协商来对部分头域进行必要的加密处理，本文提出了一种改进的 HTTP 摘要认证机制，基于此机制的 SIP 安全方案不但能够增加 SIP 系统的安全保护强度，而且可以针对不同的安全级别灵活部署。

参考文献

[1] ROSENBERG J, SCHULZRINNE H, CAMARILLO G, et al. SIP: session initiation protocol, IETF RFC3261[S]. August 2002.

[2] 娄颖.SIP 协议安全机制研究[J].广东通信技术，2005，24(4)：5-8.

[3] 龚正瑀.软交换组网与业务[M].北京：人民邮电出版社，2005：473-510.

[4] FRANKS J, BAKER P H, HOSTETLER J, et al. HTTP authentication: basic and digest access authentication, IETF RFC2617[S]. June 1999.

[5] QIU Q. Study of digest authentication for session initiation protocol(SIP)[D]. University of Ottawa, December 2003.

(收稿日期：2010-10-20)

作者简介：

彭焕峰，男，1978 年生，硕士，讲师，主要研究方向：网络通信和软件开发。