第 33 卷 第 1 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.1 Computer Engineering January 2007
·安全技术· 文章编号：1000—3428(2007)01—0151—02 文献标识码：A 中图分类号：TP309.7

现代网络安全：SIP 网络中的 DIAMETER 鉴定

达米卡
(华东理工大学计算机系，上海 200237)

摘 要：作为整个现代网络安全的基础，该文提出了验证的概念，它是会话初始化协议（SIP）网络中合并了可扩展认证协议(EAP)验证体系的一种机制。研究表明，SIP 验证可以由 EAP 验证体系进行扩展而现有的 AAA 基础结构可以为 SIP 用户再次用于验证。实施验证的过程中使用了 DIAMETER 基础协议。这个基本协议工具使用低权目录访问协议（LDAP）而且必须使用接口，DIAMETER 网络访问服务器请求（NASREQ）应用命令码的一个子集和 AVP 以在运行中实现扩展验证协议（EAP）传输。
关键词：RADIUS；DIAMETER；会话初始化协议；网络访问服务器请求；可扩展认证协议

Modern Internet Security: DIAMETER Authentication in SIP Networks

Dhammika Weerapperuma
(Department of Computer Science, East China University of Science and Technology, Shanghai 200237)

【Abstract】With undertaking the entire basis for the modern Internet security, authentication; a mechanism is proposed here which incorporates the EAP authentication framework to SIP (session initiation protocol) network. This paper shows SIP authentication can be extended via EAP (extensible authentication protocol) authentication framework and existing AAA (authentication, authorization and accounting) infrastructure can be reused for authentication of SIP users. The authentication is implemented using DAIAMETER base protocol. The base protocol tools using lightweight directory access protocol (LDAP) interface must be used, and subset of the DIAMETER NASREQ (network access server request) application command code and AVP must be used for extensible authentication protocol (EAP)transport while implementation.
【Key words】RADIUS; DIAMETER; SIP; NASREQ; EAP

全球因特网用户数仍然呈指数增长。当今个人和团体机构更关心开放式通信网络，如因特网的商业潜力。贸易及电子商务正在使用因特网并且必须寻求一条正确的途径来利用因特网。电子邮件，多媒体信息，包括 VoD(视频点播)，以及文件传输仍然为商业和信息交换的目的而使用。

安全系统要求验证来确保登录的用户确为其人。一旦用户个体登录，基于用户账号赋予的权利或者访问目标给予的特权，用户就被授权可以访问各种各样的资源。收发消息时也需要验证来检验一条特定的消息没有被虚构或在传输过程中没有被改动。因特网工程任务组(IETF)正在开发关于验证和标准的更详细的最新方法，涵盖的应用领域有电子邮件，万维网，远程登录，文档安全，多媒体会议，通用的网络工具和最为重要的电子商务。验证的技术和合法性问题涉及到许多现代化的手段，如智能卡等。

1 DIAMETER 的基础挑战

验证远端用户一直是摆在网络管理人员和 ISPs(因特网服务提供商)面前的一个巨大挑战。在这个移动通信的时代，验证机制应该做到功能强大、操作简单，只需最少的网络开销并且将全部响应次数带来的影响降至最低。IETF 的验证授权和评估(AAA)工作组已经批准把远程验证拨入用户服务(RADIUS)作为一个支持验证和授权的协议，也作为基本终端评估服务数据库使用。但大多数 ISP 认为 RADIUS 不能应付更多移动环境 SIP 网络下的问题。

考虑到 RADIUS 的不足，AAA 工作组讨论了 DIAMETER 协议。RADIUS 仅运行于标准模拟调制解调器的串行 Internet 协议和 PPP 端对端协议，而 DIAMETER 还能在无线环境下工作。RADIUS 地址空间限于 256 对，而 DIAMETER 具有一个 32 位属性值对(AVP)地址，足以应付上百万对通信进程。考虑到从远程 ISP 到用户本地代理的验证，DIAMETER 同时增强了先前 RADIUS 有限的 proxy 代理服务器能力。

2 SIP 网络

SIP 正在不断发展有协助于通过 Internet 来提供高级的 IP 服务。SIP 是 IETF 标准进程中的一部分，并且是依照其他 Internet 协议，如简单邮件传送协议(SMTP)和超文本传送协议(HTTP)的模型开发出来的。在基于 IP 的网络中，它被用来建立、修改和中断一个或多个用户间的多媒体会话或 IP 电话。为了提供 IP 服务，有若干不同的标准和协议组合在一起，特别是关于媒体传输的实时传送协议(RTP)和关于有效载荷记述的对话描述协议(SDP)，预示着当今的 IP 网络中的交互作用是为了能够保证质量，提供地址目录(LDAP)和鉴别用户(RADIUS 和 DIAMETER)。

3 网络服务器

SIP 服务器：SIP 协议意味着一个基本的网络结构模型。在 3 种不同的 SIP 服务器中，代理服务器转发请求至一个或一个以上的新目的地。图 1 显示了一个 SIP 代理服务器的情

作者简介：达米卡(1977－)，男，硕士，主研方向：网络安全
收稿日期：2006-02-28 **E-mail：**dhammika2002@yahoo.com

形。一个 proxy 代理服务器决定了该请求接下来跳往哪里，即通话路径中的下一个服务器，并且在对消息的头部信息做一些修改后进行转发。下一个服务器可以是该 proxy 代理服务器，也可以是另一个 proxy，重寄服务器，注册服务器或者是一个用户代理服务器。因此，一个请求在到达最终的目的地之前可能通过了几个 proxy 代理服务器。

DIAMETER 服务器：由 DIAMETER 客户发出 AAA 请求。DIAMETER 服务器根据习惯的 DIAMETER 应用在某一范围里受理客户的请求。如图 2 所示，DIAMETER 代理为客户和服务器提供增值服务。典型地，DIAMETER 客户端是一个网络访问服务器(NAS)，为一个特定的访问技术提供 AAA 服务。NAS 在分配网络资源之前需要鉴别连入网络的终端，如允许访问前先验证用户的身份。

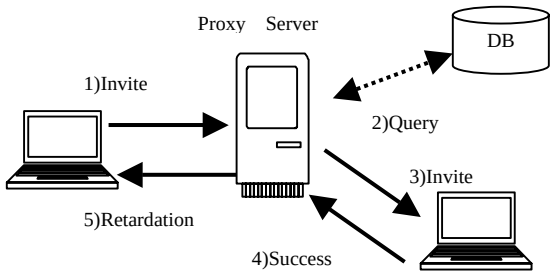


图 1 SIP 代理服务器

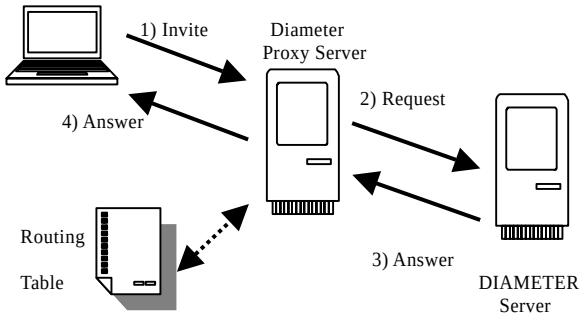


图 2 Diameter 代理服务器

4 SIP 网络中 DIAMETER 验证的实行

网络体系结构由几个独立的域组成，具有 DIAMETER 和 SIP 基础结构如图 3 所示。域的负责人控制着该域中策略的执行情况；有一种已定义的服务，对某一域就如同整个网络一样提供独一无二的服务。

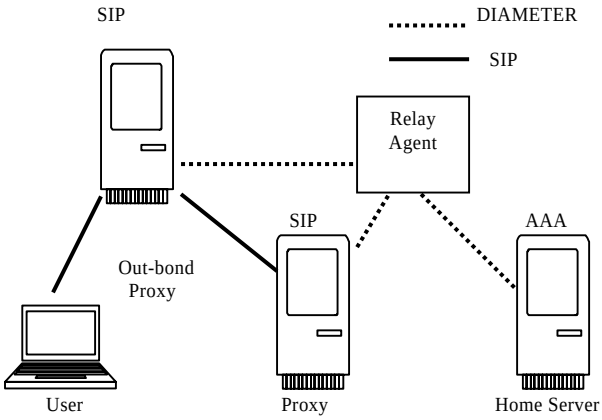
体系结构中最为关键的是每个域都存在一个 SIP 实体管理着该域的地址记录；以及一个 DIAMETER 实体负责该域的网络访问检验(NAI)。有若干网络要素对应于管理部分，或是使用这些管理部分。

用户代理是在域负责人处设立了用户账号优先权的 SIP 终端。用户账号由一个 SIP 地址记录和一个 NAI 组成。通常这两部分是相同的，但也有可能不一样。那种情况下，用户的 DIAMETER 主服务器和 SIP 注册服务器可能在两个域中。

位于一个域的边缘处的边界 proxy 代理服务器执行 SIP 策略。它根据应用层的信息来确定 SIP 消息的传输路径，通常接近本地组织，例如，防火墙或一个网络地址解析器。边界代理的运作与普通代理类似。

代理/注册服务器实体在域的 AAA(DIAMETER)的帮助下管理着一个域的地址记录。proxy 代理实体利用注册服务器提供的信息，为去往该域地址记录中任何地方 SIP 消息确定路径。注册服务器从用户代理处收集地址，那里存在一个有效的用户账户。

中继代理实体是域 AAA 基础结构的一部分。它利用应用层的信息来确定 DIAMETER 消息的传输路径。当然，网络中也可能存在其他 DIAMETER 代理，例如，proxy 代理、重寄代理、转换代理。



Mobile user：移动用户；Out bound proxy：边界代理服务器；
Proxy/registrar proxy：代理/注册服务器；
Relay agent：中继代理；Home server：主服务器。

图 3 SIP DIAMETER 体系结构

主服务器是受理去往域里的所有 AAA 请求的 DIAMETER 服务器。主服务器最终控制了域里的 NAI。

DIAMETER 请求也可以从其他域发出，这样就有另一种不同类型的授权和评估服务。

5 方法和结果

实施验证的过程中使用了 DIAMETER 基础协议。这个基本协议工具使用低权目录访问协议(LDAP)而且必须使用接口，DIAMETER NASREQ(网络访问服务器请求)应用命令码的一个子集和 AVP 在运行中实现扩展验证协议(EAP)传输。所有的组成部分主要由软件构成：相应于 SIP UA 的 SIP 用户代理(UA)；相应于 SIP proxy 代理/注册服务器的双重代理；AAA 服务器，DIAMETER 服务器。

表 1 响应编码对应结果

Request IP	DIAMETER Result-Code Identity: 202.8.0.xxx		SIP Event		Event Description
	Code	Description	Code	Description	
202.8.0.1	1001	Diameter multi round authentication	401	Unauthorized	Bearer capability not authorized
202.8.0.1	2001	Diameter success	200	OK	Normal
202.8.0.1	3002	Diameter unable to deliver	500	Unauthorized	Temporary Failure
202.8.1.1	4001	Diameter authentication rejected	403	Forbidden	Bearer capability not authorized

增加 SIP－UA 的同时附加了 SIP—EAP 验证机制，SIP—EAP 验证者提供 EAP 验证功能，且 GUI 的扩展功能为特定的 EAP 过程提供了一个密码对话框。增加双重 proxy 代理的同时附加了 SIP—EAP 验证，SIP—EAP 验证机制用于提供 EAP 分解和 AAA 技术支持。LDAP 接口仅用于双重 proxy 代理中。

这里 AAA 服务器再次将低权目录访问协议(LDAP)接口技术用于共享保密存储内容，为了在主服务器中增加 DIAMETER NASREQ 和 EAP 支持技术而增加了 EAP 服务器

（下转第 169 页）