一种基于 EAP-SAKE 的分层 Web 安全模型

张建伟,贺 蕾
ZHANG Jian-wei,HE Lei

郑州轻工业学院 计算机与通信工程学院,郑州 450002
School of Computer and Communication Engineering,Zhengzhou University of Light Industry,Zhengzhou 450002,China
E-mail:ing@zzuli.edu.cn

ZHANG Jian-wei,HE Lei.Layered Web security model based on EAP-SAKE.Computer Engineering and Applications, 2008,44(18):97-98.

Abstract: With the development and application of Web service technology,the Web security issues are increasingly prominent.It is proposed a layer security model and security mechanism to implement this model based on the EAP-SAKE for the Web.This model has the advantages of flexibility and extensibility,reduces the complexity of the system,and provides the various keys in different layers.It satisfies the security requirement of the Web service.

Key words: layered model;EAP-SKAE;key;Web security

摘 要: 随着 Web 服务技术的应用与发展,Web 安全问题日益突出。针对 Web 服务应用模式,提出了一种分层 Web 安全模型,以及基于 EAP-SAKE 的实现该模型的安全机制。该模型具有灵活性和可扩展性,降低了系统的复杂性,并提供了不同层次的密钥以供使用,满足了 Web 服务的安全需求。

关键词: 分层模型;EAP-SAKE;密钥;Web 安全
DOI: 10.3778/j.issn.1002-8331.2008.18.030 **文章编号:** 1002-8331(2008)18-0097-02 **文献标识码:** A **中图分类号:** TP309.2

1 引言

Web 服务技术是当前基于 Web 的分布式技术与应用的关键技术基础。随着 Web 服务技术的日益成熟,众多基于 Web 的分布式应用系统都选择了具有简单性、标准性和可互操作性的 Web 服务技术作为其实现的关键技术基础,而安全通信则是 Web 服务在 Internet 上得到广泛应用的基础。

由于 Web 服务通信以 SOAP(Simple Object Access Protocol)消息的传输为基础,而 SOAP 协议是应用层协议,因此Web 服务安全通信必须保证应用层 SOAP 消息的安全,并同时满足 Web 服务应用提出的一些特殊需求,如对消息进行局部加解密等。如何提供安全可信的 Web 服务,保证 Web 服务的通信安全,已成为 Web 服务进一步推广和应用必须解决的关键问题。为解决 Web 应用中的安全问题,一些学者提出了分层的 Web 安全模型。如李冬等提出了一种基于 XML 的面向 Web 服务的分层安全模型,但该模型中并没有明确定义密钥的产生方式。针对这点不足,本文提出了一种 Web 分层安全模型,以及基于 EAP-SAKE 的实现该模型的安全机制,重点解决了该分层模型中的密钥协商问题。

2 Web 分层安全模型

2.1 分层安全模型

Web 安全层次模型是一种面向服务的可信 Web 服务安全模型,其总体结构如图 1 所示。该模型包括了 3 个层次:原始数据层、安全层和应用层。原始数据层产生标准的 XML 文档,安全层实现各种安全措施,为应用层实现其安全目标提供支持。

根据安全措施的功能,安全层被划分为 2 个子层:安全服务子层和通信安全子层。其中,安全服务子层提供诸如加密、解密、签名、认证等复杂的 PKI 系统功能,确保数据和消息的机密性、完整性、抗抵赖性等。安全通信子层负责协商密钥,并对传输的 SOAP 消息进行保护。需要说明的是,安全层的 2 个子层并不构成严格的上下层关系,在实际应用中,它们也可能是相互交叉、相互支持的关系。

2.2 通信安全子层安全机制

在通信安全子层中,采用基于 EAP-SAKE(Extensible Authentication Protocol-Shared-secret Authentication and Key Establishment)的报文交换机制进行报文交换,并协商产生密钥。在进行报文交换前,通信节点和服务器首先要共享一个 Root-Secret,并将其分成两个密钥,分别是 16 byte 的 Root-Secret-A

基金项目: 国家重点基础研究发展规划(973)(the National Grand Fundamental Research 973 Program of China under Grant No.2007CB307102);河南省教育厅自然基金(the Natural Science of Foundation of Education Department of Henan Province of China under Grant No.20065,20019)。

作者简介: 张建伟(1971-),男,博士研究生,副教授,主要研究领域为网络与信息安全技术;贺蕾(1980-),男,助教,主要研究领域为无线网络信息安全。

收稿日期: 2007-09-17 **修回日期:** 2008-01-07

和 16 byte 的 Root-Secret-B。Root-Secret-A 主要用于进行认证和生成 TEK(Transient EAP Keys),Root-Secret-B 主要用来计算 MSK(Master Session Key)和 EMSK(Extended Master Session Key)。Root-Secret-A 和 Root-Secret-B 必须是相互独立的。报文交换过程如图 2 所示。

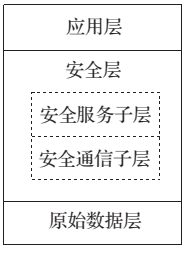

图 1 Web 安全层次模型

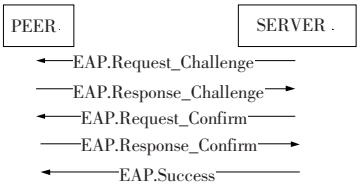

图 2 EAP-SAKE 的报文交换机制

首先,服务器发送 EAP.Request_Challenge 报文,该报文中包括 AT_RAND_S 和 AT_SERVERID。其中,AT_RAND_S 的值是服务器生成的随机数;AT_SERVERID 是服务器的身份标识符。

通信节点收到服务器发送的 EAP.Request_Challenge 报文后发送 EAP.Response_Challenge 报文,该报文中包括 AT_RAND_P、AT_PEERID、AT_SPI_P 和 AT_MIC_P。其中,AT_RAND_P 的值是通信节点生成的随机数,AT_PEERID 是通信节点的身份标识符,AT_SPI_P 是通信节点所支持的密文族,AT_MIC_P 是完整性校验码。然后通信节点使用 AT_RAND_S、AT_RAND_P 和 Root-Secret-A 计算出 SMS(SAKE Master Secret)和 TEK(Temporary EAP Keys),并利用 AT_RAND_S、AT_RAND_P 和整个 EAP 报文计算完整性校验码 AT_MIC_P。

服务器收到通信节点发送来的 EAP.Response_Challenge 报文后,用同样的办法计算出 SMS 和 TEK,以及完整性校验码,并将计算结果与收到的 AT_MIC_P 进行比较,如果相同,就认为通信节点通过了认证。服务器从通信节点发送的 AT_SPI_P 中选择适当的加密算法和参数,对通信数据进行加密。服务器发送的 EAP.Request_Confirm 报文包括 AT_SPI_S、AT_ENCR_DATA 和 AT_MIC_S。其中,AT_SPI_S 是服务器选择的密文,AT_ENCR_DATA 包含的是加密后的信息,AT_MIC_S 是完整性校验码。

通信节点收到服务器发送的 EAP.Request_Confirm 报文后认为服务器已经通过了对它的认证。通信节点采用同样的方法计算完整性校验码,将计算结果与 EAP.Request_Confirm 报文中的 AT_MIC_S 进行比较,如果相同,就认为服务器通过了认证。然后发送 EAP.Response_Confirm 报文。其中包括完整性校验码 AT_MIC_P。

服务器收到 EAP.Request_Confirm 报文后,发送 EAP.Success 报文给通信节点,结束 EAP 会话。

EAP-SAKE 中的密钥共分为 3 个等级,第 1 等级是 Root Secret,包括 Root-Secret-A 和 Root-Secret-B part;第 2 等级是 SMS,用于生成第 3 等级的密钥;第 3 等级是会话密钥,包括 TEK、MSK(Master Session Key)和 EMSK(Extended MSK)。不同的密钥在分层中的应用如图 3 所示。

图 3 密钥在安全层中的应用

2.3 安全服务子层安全机制

安全服务子层使用安全通信子层协商得出的 TEK、MSK 和 EMSK 等密钥进行加密、解密、签名、认证等复杂的 PKI 系统功能,也可以根据需要添加其他安全模块,以确保数据的机密性、完整性、抗抵赖性等。其中 TEK 又进一步分为两个密钥 TEK-Auth 和 TEK-Cipher,TEK-Auth 用来实现签名、认证、完整性校验等功能,TEK-Cipher 用来进行加解密,以实现对消息进行局部加解密等功能。MSK 和 EMSK 则用来实现对转发消息进行加解密等功能。

3 模型特点

该模型具有以下优点:

(1)分层模型可以根据不同的应用需求选择不同的安全组件,提高了系统的灵活性;

(2)分层模型具有良好的可扩展性。新的安全技术和规范可以很方便地融入该模型;

(3)分层模型可以降低系统的复杂性,应用层只需要实现系统功能即可,由安全层实现所有的安全措施;

(4)采用基于 EAP-SAKE 的安全机制可以协商出不同层次的密钥,方便用户根据需要灵活选用,并且有利于密钥的保密。

4 结束语

安全是 Web 服务得以广泛应用的基础。本文提出了一种分层的 Web 安全模型,并在此基础上重点研究了该模型中的安全通信子层,设计了一种基于 EAP-SAKE 的安全机制。通过引入分层安全模型,解决了典型 Web 服务应用模式下的通信安全问题,降低了提供安全服务的系统复杂性,提高了系统灵活性和可扩展性。今后工作的重点将放在更为复杂的 Web 综合服务的应用场景,即研究在多业务融合下的 Web 安全。

参考文献:

[1] Blunk L,Vollbrecht J.RFC2284,PPP Extensible authentication protocol[S].1998.

[2] Vanderveen M,Soliman H.RFC4763,extensible authentication protocol method for shared-secret authentication and key establishment[S].2006.

[3] 李冬,郭荷清,韩涛.一种面向 Web 服务的分层安全模型[J].计算机工程与设计,2006,27(20):3766-3767.

[4] 孟伟,张璟,李军怀,等.Web 服务安全模型研究与实现[J].计算机工程与应用,2006,42(26):134-136.

[5] 陈大沟,严毅.Web 服务安全性分析[J].广西大学学报,2005,30(8):78-80.