域密钥识别邮件技术综述

王昕溥[1,2], 姚健康[1], 李晓东[1], 王 峰[1], 毛 伟[1]
(1. 中国科学院 计算机网络信息中心, 北京 100080; 2. 中国科学院 研究生院, 北京 100049)

摘 要: 介绍了 DKM的基本概念和框架结构,分析了 DKM的工作原理,并且重点讨论了 DKM面临的威胁以及发展前景。

关键词: 域密钥识别邮件; 垃圾邮件; 域名; 认证
中图分类号: TP393. 08 **文献标志码**: A **文章编号**: 1001-3695(2008)01-0033-04

Survey of domain keys identified mail

WANG Xin-pu[1,2], YAO Jian-kang[1], LI Xiao-dong[1], WANG Feng[1], MAO Wei[1]
(1. *Computer Network Information Center, Chinese Academy of Sciences, Beijing* 100080, *China*; 2. *Graduate School, Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: This paper introduced the conception and framework of DKM, expatiating the working flow with examples and discussed threats and the prospect of DKM.

Key words: DKM (domain keys identified mail); spam mail; DNS; authentication

随着互联网的发展,电子邮件早已成为人们彼此互通信息最主要的工具之一。然而目前垃圾邮件约占据全部邮件总数的 88%之多。其所引发的网络频宽负荷,以及病毒、网络钓鱼攻击等事件的严重性是非常巨大的。由于垃圾邮件多半采用隐藏真实发信来源地址的技术,不但很难找出真正的来源地址,而且垃圾邮件发信者常常冒用许多公司、银行的名义来发送内藏有网络钓鱼 (phishing)或后门程序 (backdoor)的垃圾邮件,造成个人重要信息被窃取,甚至沦为垃圾邮件发送僵尸以及远端遥控的跳板。在这种情况下,电子邮件验证技术就显得尤为重要。本文所介绍的 DKM技术就是其中的一种。

背景与基本概念

一直以来,许多知名厂商均在建立电子邮件验证技术。其中最著名的包括 Yahoo的 DomainKeys技术、微软的 SenderID技术与思科系统的 identified internet mail技术。其中,DomainKeys技术受到 SBC、英国电信与 Google Gmail的支持;而 MSN Hotmail、AOL、美国银行及 eBay皆响应 SenderID技术。微软曾一度打算说服 IETF工作小组通过 SenderID技术成为业界标准,最后却因为各家担心全球通用的技术为一家完全垄断而使微软的愿望落空。如今,由 Yahoo与思科系统合作发表的 DKM技术,既结合两家各自的技术,也不会有垄断于一家的争议。DKM技术是现阶段在 IETF内部讨论的方案,并且有望在今后成为国际标准。

域密钥识别邮件定义了一种机制,通过对邮件信息加密并签名,从而允许实施签名的域名对将该邮件引入邮件传输流负责[1]。邮件接收者可以通过直接查询签名者的域名得到相应的公共密钥,进而校验邮件的签名,以此验证邮件是否属于拥有签名域名的私有密钥的一方。DKM允许一个机构对邮件负责。这个负责的机构是一个邮件传输过程中的处理者,可以是邮件的发起者或中介。负责的机构在邮件中添加一个数字签名,并把这个签名与机构的一个域名相关联。通常,签名会由一个服务代理在邮件发起人的行政管理域 (ADMD)的授权下,由这个环境中的任何一个功能组件来执行,包括邮件客户端 (MUA)、邮件提交代理 (MSA)、网界邮件传输代理 (MTA)。DKM也允许签名由授权第三方来进行。邮件签名后,在邮件传输途径中的任何代理均可被选择用来执行对签名的验证。通常验证会由邮件接收者的行政管理域代理完成。与签名时相同,可以由这个环境中的任何功能组件来完成。特别地,这样意味着签名可以由邮件接收者的行政管理域的过滤软件来处理,而不是要求邮件接收者的用户终端来进行判断。用来进行数字签名的域名所有者是以其信誉为基础的。接收者成功验证签名后可以利用签名者的身份信息作为限制垃圾邮件、欺骗、钓鱼网站或其他不受欢迎行为的软件的一部分。

特点

基于对 DKM概念的介绍,可以发现 DKM利用以下几点定义了一个邮件认证机制:公共密钥加密、基于 DNS的公共密钥发布服务、域名标志符。

DKM所采用的途径与传统的邮件签名方法 (如 S/MIME[2]、OpenPGP[3])相比,有以下一些主要特点:

a) DKM不修改邮件正文,而是将邮件签名参数信息放在一般不显示给接收者的邮件头部。S/MIME和 OpenPGP同时要求对邮件正文进行修改,将正文部分作为 MIME类型进行封装。因此签名邮件对于软件不支持 DKM的终端用户是透明

收稿日期: 2007-02-07; **修回日期**: 2007-04-15

作者简介:王昕溥 (1984-),男,辽宁大连人,硕士,主要研究方向为计算机网络应用技术、计算机网络 (wangxinpu@cnnic.cn);姚健康 (1978-),男,硕士,主要研究方向为计算机网络应用技术;李晓东 (1976-),男,博士研究生,主要研究方向为计算机网络资源寻址技术;王峰 (1977-),男,博士研究生,主要研究方向为计算机网络应用技术;毛伟 (1968-),男,主任,研究员,硕导,博士,主要研究方向为计算机网络系统、互联网寻址技术.

的,而不像 S/MIME和 OpenPGP由于修改了正文会造成邮件内容在不支持协议的客户端上无法识别。

b)没有对分发公有/私有密钥对的可信证书权威的依赖。签名程序要求一定级别确保验证时采用的公共密钥是与声称的签名者相关联。许多程序通过一个可信第三方的证书授予来实现这一点。但是由于 DKM的使用范围有限,并不需要通用的、强大的、长期的由独立权威颁发的证书。DKM通过使验证者简单地向签名者的 DNS发出查询来获取公共密钥,实现了一个足够的安全级别。这样就使得它使用的成本更低。

c)没有对任何新的有关公共密钥分发撤回的互联网协议或服务部署的依赖。现在已经定义的是一种单一绑定的利用 DNS TXT记录来分发密钥,其他的方式可能会在以后被定义。

d)DKM是基于域名的,而不是整个邮件地址。签名是由域名的管理者控制而不是单独的邮件用户。

e)签名的校验失败不会导致邮件被拒绝。DKM没有规定收件人必需的操作,可以将对邮件的判断提交给邮件过滤的其他组件。

f)机制中不包括加密算法。DKM支持多种数字签名算法。目前主要采用的是 RSA-SHA[4,5]。可以随着算法的进步而采用新的加密算法。

g)存档并不是设计目标。DKM是为了满足邮件传输认证的短期需求。

架构

图 1给出了 DKM系统的基本框架。首先签名者需要在相应的代理处增加代码执行签名并且需要修改 DNS管理工具以允许创建 DKM密钥记录。被签名的邮件通过网络传输到验证者。验证者需要在相应的代理处增加代码执行验证并且将结果提供给邮件部署系统需要的部分,如过滤引擎。因为仅仅是经过验证的签名并不能够表示邮件是可以接收的,仍然需要转送给其他评估阶段。在评估阶段签名的有效性以及签名域名的信誉均可能成为评估的条件,但是 DKM并不对评估行为进行定义。

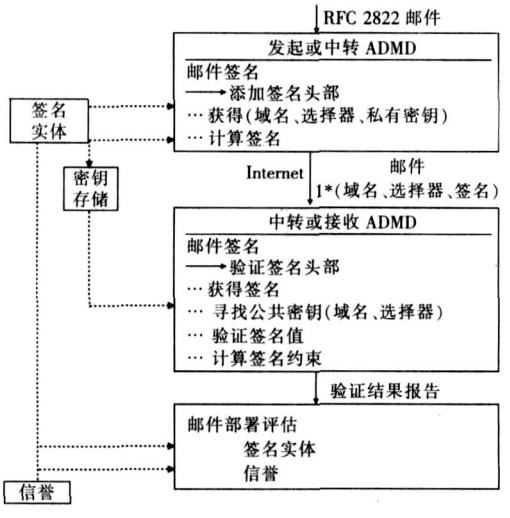

图 1 DKIM 系统框架

邮件的签名储存在 DKM-Signature头部域。这个部分包括所有的签名以及提供给验证者获取密钥的相关属性。

在 DKM签名部分包括的主要属性信息有 a表示产生签名所采用的算法; i表示用户或者代理的标志符; c表示正文规范化的方法; d表示签名实体的域名; s表示选择器用来细分域名; h表示在邮件头中选定的用于产生签名的部分; l表示选去邮件正文的截断长度; b表示邮件头部数字签名的内容; bh表示邮件数字签名的内容; q表示得到公共密钥的查询方式。

. 签名者动作

1)判断邮件是否应该加密 签名者只应该对含有私有公有密钥对以及选择器信息的域名所负责的邮件加密。除了缺少上述条件外,也有一些其他的原因使得签名者选择不对邮件签名。

2)选择一个私有密钥和相应选择器 选择器用来在同一个管理域名下实现多重密钥。这可以给为域名拥有者工作的部门、数据区域或第三方提供各自的签名管理。验证者利用选择器作为一个附加的域名部分,用来划分 DNS查询的域名。在同一个域名下,不同的选择器代表不同的 DKM DNS记录。DKM并不规定签名者应该根据什么来选择哪个密钥和选择器信息。就目前来讲,DKM规范对待所有的选择器都是一样的。所以采用选择器时考虑的重点可能是管理上的方便。在加密者对邮件头的选定部分利用私有密钥加密之后,一个选择器被指定为 DKM签名的一个属性记录在 DKM签名的头部域,用来向验证者提供找到 DKM的公共密钥的信息。

3)规范化 对于一些邮件,尤其是使用 8 bit字符的邮件,在传输过程中容易被修改,如被转换成 7 bit的形式。这种转换会破坏 DKM签名。为了将这种破坏的可能性最小化,签名者应该在签名前将邮件内容转换成一种合适的 MIME传输编码[6]。实际上这种转换并不是 DKM的范畴,而是应该在邮件传送给 DKM算法之前由 MUA或 MSA进行处理。

如果传送给签名者的邮件包含任何在传输过程中会被修改的本地编码,那么在签名前必须进行规范化修改[7]。特别是单独的 CR或 LF(有些系统中用于本地换行符)必须在签名之前转换为 SMTP标准的 CRLF序列。对于修改有两种不同的态度。对大多数签名者,适度地修改邮件对于邮件认证有效性的状态不会有实质性的影响,因此签名者倾向于采用能够经受传输中适当修改的规范化算法。其他一些签名者要求对邮件的任何修改均会导致签名的认证失败。这样的签名者要采用的签名算法不能容忍签名邮件在传输过程中的任何修改。一些签名者可能会接收在邮件标准下[7]对邮件头部域的修改但是不愿意接收对邮件正文的任何修改。

为了满足各种需求,邮件头部和邮件正文定义了两种规范化算法。一种简单算法不允许传输过程中对邮件作任何修改; 另一种不严格算法允许普通的修改,如空格的替换和邮件头部的重新封装。签名者可以对邮件头部或正文指定任意一种规范化算法,如果没有指定,邮件头部和正文的简单算法为默认。

签名者可以选择签名邮件正文的长度。实际上进行签名的邮件正文长度应插入到 DKM签名头部的 l属性中。因此在规范化中,签名者根据 c属性中指定的算法和 l属性中指定的截断长度来进行规范化。规范化只是用来对邮件内容进行调整以方便签名或验证,而并不对邮件的传输产生任何影响。

4)决定邮件头部要加密的部分 邮件头部的 from域是必须被签名的; 同时可以选择任何其他在签名时存在的头部域。签名者不应该对有可能在传输过程中被合法修改和去除的域进行签名,尤其是在邮件协议中被明确允许修改或去除的 return-path邮件头部域[8]。

DKIM签名头部域隐含规定为必须被签名的,并且不能被添加在 h属性中。除非为了表明其他已经存在的 DKIM签名也再次被签名。签名者可以声称对不存在的邮件头部域进行了签名(在 h属性中包含的邮件头部域在邮件中并不存在)。当计算签名时,不存在的邮件头部域必须被当做空字符串来处理。

5)签名　签名邮件签名的第一步是通过 hash算法计算邮件的两个 hash值。一个是对邮件正文;另一个是对邮件头部选择的部分。签名者必须按照这个顺序计算 hash值,而验证者可以按照任意方便的顺序。首先,签名者对规范化后的邮件正文进行 hash,其结果被转换为 base64形式插入到 DKIM签名头部的 bh属性;然后,签名者根据 h属性所指定的要进行签名的邮件头部域以及顺序,对已经规范化的邮件头部进行 hash,以 base64形式插入到 b属性。签名者第二步通过选定的 RSA算法(实际上是 PKCS#1[9])采用签名者的私有密钥对得到的 hash值进行加密签名。

6)插入 DKIM签名头部　签名者必须在传输邮件之前插入 DKIM签名头部域。关键字 DKIM-Signature必须在所有 DKIM签名属性插入前写入邮件头部。

. 验证者动作

1)确认签名头部域　验证者必须确认 DKIM签名头部域的格式和值的有效性。如果存在任何不一致和未知数值以及缺少必需的属性,头部域均会整体被忽略并且验证者返回 PERMFAIL(签名语法错误)。但是在 DKIM签名头部域存在未知的额外属性是允许的。

2)获得公有密钥　验证签名需要得到签名的公共密钥。获得公共密钥的方法依赖于 DKIM签名头部域中的 q属性定义的查询类型。目前主要是查询签名者域名的 TXT RR记录。

密钥查询算法的参数是查询类型(q属性)、签名者的域名(d属性)和选择器(s属性):public_key = dkim_find_key(q_val, d_val, s_val)[1]。

3)计算验证　给定一个签名者和公共密钥。验证首先根据 c属性定义的规范化算法、l属性定义的邮件正文签名长度和 h属性定义的邮件头部签名部分,对邮件进行规范化处理。根据 a属性定义的算法以及得到的公共密钥,计算规范化后的邮件加密 hash值;然后验证邮件正文的加密 hash值是否与 bh属性所传递的 hash值相同。类似地,利用 a属性定义的算法和公共密钥值,根据邮件头部的 hash值验证 b属性传递的签名。

4)传递验证结果　验证者希望通过任何合适的方法将验证结果传递给邮件系统的其他部分。比如在向邮件添加一个邮件头部。所有这种头部应该插入到任何存在的 DKIM签名或已经存在的验证状态头部域之前。

举例

用一个例子来简单介绍 DKIM的流程。原始邮件头如下:

```
From: Simple W <simple@football.example.com>
To: Julyseven X <julyseven@shopping.example.net>
Subject: Je t'aime
Date: Wed, 18 Oct 2006 21:00:00-0700 (PDT)
Message-ID: <20061018040037@football.example.com>
```

加密传输后,在邮件头部添加了 DKIM签名域,验证者得到的邮件头如下:

```
From: Simple W <simple@football.example.com>
To: Julyseven X <julyseven@shopping.example.net>
Subject: Je t'aime
Date: Wed, 18 Oct 2006 21:00:00-0700 (PDT)
Message-ID: <20061018040037@football.example.com>
DKIM-Signature:
 a=rsa-sha256; s=dalian; d=example.com; c=simple; q=dns/txt;
 i=simple@football.example.com;
 h=Received: From: To: Subject: Date: Message-ID;
 bh=ZSVEYuq4ri3LR9S+qjlzCP+LxvJrIfiO12g5hxp5+MI=;
 b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+
yuU4zGeeruD00lszZVoG4ZHRNiYzR;
Received: from dsl-10.2.3.4.football.example.com [10.2.3.4]
  by server.example.com with SUBMISSION;
  Wed, 18 Oct 2006 21:00:45-0700 (PDT)
```

在这个例子中,验证程序利用从"d="标记中提取的域名"example.com",以及从"s="标记中提取的选择器"dalian"形成了一个 DKIM查询:dalian._domainkey.example.com。

签名的验证结果储存在"Authentication-Results"头部中。经过验证成功,邮件被转换成:

```
X-Authentication-Results: shopping.example.net
 header.from=simple@football.example.com; dkim=pass
Received: from mout23.football.example.com (192.168.1.1)
 by shopping.example.net with SMTP;
DKIM-Signature:
 a=rsa-sha256; s=dalian; d=example.com; c=simple; q=dns/txt;
 i=simple@football.example.com;
 h=Received: From: To: Subject: Date: Message-ID;
 bh=ZSVEYuq4ri3LR9S+qjlzCP+LxvJrIfiO12g5hxp5+MI=;
 b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+
yuU4zGeeruD00lszZVoG4ZHRNiYzR;
Received: from dsl-10.2.3.4.football.example.com [10.2.3.4]
 by server.example.com with SUBMISSION;
 From: Simple W <simple@football.example.com>
 To: Julyseven X <julyseven@shopping.example.net>
 Subject: Je t'aime
 Date: Wed, 18 Oct 2006 21:00:00-0700 (PDT)
 Message-ID: <20061018040037.46341.5F8J@football.example.com>
```

5　DKIM面临的威胁和发展前景

就像其他任何试图阻止垃圾邮件传播的机制一样,DKIM也会受到各种攻击。一方面有针对 DKIM协议本身的攻击,比如错误的邮件长度限制(l属性)、错误的私有密钥、DKIM签名头部域格式错误等无意或有意的属性赋值错误,均可能造成的认证失败;另一方面,DKIM机制所依赖的 DNS服务本身也具有很多不安全的因素[12]。各种针对 DNS的攻击均有可能使得 DKIM签名失效甚至被伪造。对于这些可能的攻击,DKIM工作组发表了针对各种攻击行为的分析[10]。如何完善 DKIM协议以应对对于协议本身的攻击也是 DKIM今后改进的重要内容。对于通过 DNS服务所进行的攻击,已经超出了 DKIM本身所考虑的范畴。因此 DKIM一方面寄希望于 DNSSEC[13]的出现和使用解决现有的一部分问题;另一方面 DKIM的设计初衷认为各种通过 DNS的针对 DKIM的攻击行为相对于攻击建立在 DNS基础上的其他应用成本高且回报很少。想要系统性地威胁 DKIM的设计目标,攻击者必须在 DNS服务的多个部分进行长时间高成本的攻击。这种行为的非经济性会在某种程度上阻止对 DKIM的攻击。

DKIM只是为了实现一定程度上足够的认证,而并不是为了提供一种强大的加密认证机制[10]。这种在安全性上的不完全可靠,对于网络钓鱼等涉及隐私程度高可能造成巨大损失的

欺骗行为,DKM所得出的结论是具有风险和不可信赖的。因此 DKM的主要应用前景是在即使被攻击或认证失败也不会有很大损失的反垃圾邮件等低危险性领域。在反垃圾邮件方面,DKM能够有效地限制垃圾邮件发送者盗用其他机构或域名的名义,为邮件过滤提供鉴别手段,并且能够在现有邮件体系下快速进行低成本的部署。IETF DKM工作组正在致力于完善 DKM协议,积极推动 DKM草案成为正式的 RFC标准,并且已经取得了阶段性的成果。在开发部署上面,已经有 Sendmail、Postfix、Apache等多家公司和组织参与开发了可用的稳定版本,并且正在继续进行改进和标准化工作。

结束语

本文以基于 DKM的框架结构为主,分析了 DKM技术的概念、流程和发展趋势。虽然 DKM技术还处在发展中,尚未形成标准,但是它已经能够在反垃圾邮件的工作中起到一定的积极作用,值得关注。国内目前关于 DKM的介绍还不是很多,希望本文系统化的介绍和分析能够对反垃圾邮件工作提供一些参考。

参考文献:

[1] ALLMAO E, CALLAS J, DELAOY M, *et al* Domain keys identified mail(DKIM) signatures[S]. [S. l]: IETF, 2006.

[2] GALVIN J, MURPHY S, CROCKER S, *et al* RFC 1847, Security multiparts for MIME: multipart/signed and multipart/encrypted[S]. [S. l]: IETF, 1995.

[3] CALLAS J, DONNERHACKE L, FINNEY H, *et al* RFC 2440, OpenPGP message format[S]. [S. l]: IETF, 1998.

[4] National Institute of Standards and Technology. NIST FIPS PUB 186: digital signature standard[S]. [S. l]: Department of Commerce, 1994.

[5] RIVEST R L, SHAMIR A, ADLEMAN L M. A method of obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[6] FREED N, BORENSTEIN N. RFC 2045, Multipurpose Internet mail extensions (MIME) part one: format of Internet message bodies[S]. [S. l]: IETF, 1996.

[7] RESNICK P. RFC 2822, Internet message format[S]. [S. l]: IETF, 2001.

[8] KLENSIN J. RFC 2821, Simple mail transfer protocol[S]. [S. l]: IETF, 2001.

[9] JONSSON J, KALISKI B. RFC 3447, Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1[S]. [S. l]: IETF, 2003.

[10] FENTON J. RFC 4686, Analysis of threats motivating domain keys identified mail (DKIM)[S]. [S. l]: IETF, 2006.

[11] HANSEN T, CROCKER D, HALLAM-BAKER P. DomainKeys identified mail(DKIM) service overview[S]. [S. l]: IETF, 2006.

[12] ATKINS D, AUSTEIN R. RFC 3833, Threat analysis of the domain name system (DNS)[S]. [S. l]: IETF, 2004.

[13] ARENDS R, AUSTEIN R, LARSON M, *et al* RFC 4033, DNS security introduction and requirements[S]. [S. l]: IETF, 2005.

[14] THOMAS M. Requirements for a DKIM signing practices protocol [S]. [S. l]: IETF, 2006.

[15] ALLMAN E, DELANY M, FENTON J. DKIM sender signing practices [S]. [S. l]: IETF, 2006.

(上接第 32页)

[2] FELDMAN R, DAGAN I. Knowledge discovery in textual databases (KDT)[C]//Proc of the 1st Int'l Conf on Knowledge Discovery and Data Mining. Montreal: [s. n.], 1995: 112-117.

[3] CHAKRABARTI S. Data mining for hypertext: a tutorial survey[J]. SIGKDD Exploration, 2000, 1(2): 1-11.

[4] COOLEY R, MOBASHER B, SRIVASTAVA J. Web mining: information and pattern discovery on the World Wide Web[C]//Proc of the 9th Int'l Conf on Tools with Artificial Intelligence. Washington DC: IEEE Computer Society Press, 1997: 558-567.

[5] MADRIA S K, BHOWMICK S. Research issue in Web data mining [C]//Proc of the 1st Int'l on Data Warehousing and Knowledge Discovery. Canada: AAAI Press, 1999: 303-312.

[6] PITKOW J. In search of reliable usage data on the WWW[C]//Proc of the 6th Int'l World Wide Web Conference. Santa Clara: Elsevier Science, 1997: 133-142.

[7] GRAHAM-CUMMING J. Hits and misses: a year watching the Web [C]//Proc of the 6th Int'l World Wide Web Conference. Santa Clara: Elsevier Science, 1997: 118-123.

[8] PERKOWITZ M, ETZIONI O. Adaptive Web sites: conceptual cluster mining[C]//Proc of the 16th International Joint Conference on Artificial Intelligence. Stockholm: [s. n.], 1999: 344-349.

[9] SRIVASTAVA J, COOLEY R, DESHPANDE M. Web usage mining: discovery and applications of usage patterns from Web data[J]. SIGKDD Explorations, 2000, 1(2): 12-23.

[10] SHAHABI C, ZARKESH A, ADIBI J, *et al* Knowledge discovery from users Web-page navigation[C]//Proc of IEEE RIDE Workshop. Los Alamitos: IEEE Computer Society Press, 1997: 204-210.

[11] LUOTONEN A. The common log file format [EB/OL]. (1995-09-27). http://www.w3.org/pub/www/.

[12] FastStats log analyzer [EB/OL]. (1999-06-12). http://www.mach5.com/fast/.

[13] ZAIANE O, XIN M, HAN J. Discovering Web access patterns and trends by applying OLAP and data mining technology on Web logs [C]//Proc of Advances in Digital Libraries Conference (ADL). Sante Barbara: [s. n.], 1998: 19-29.

[14] BUCHNER A, MULVENNA M D. Discovering Internet marketing intelligence through online analytical Web usage mining[J]. SIGMOD Record, 1998, 27(4): 54-61.

[15] MDBASHER B, COOLEY R, SRIVASTAVA J. Automatic personalization based on Web usage mining[J]. Communications of the ACM, 2000, 43(8): 142-151.

[16] MOBASHER B. Grouping Web page references into transactions for mining World Wide Web browsing patterns[C]//Proc of IEEE Knowledge and Data Engineering Exchange Workshop. New York: IEEE Press, 1997: 108-132.

[17] COHEN E, DATAR M, FUJIWARA S. Finding interesting associations without support pruning[J]. Communications of ACM, 2002, 49(8): 122-131.

[18] ZAIANE O R, HAN J. Resource and knowledge discovery in global information systems: a preliminary design and experiment[C]//Proc of the 1st Int'l on Knowledge Discovery and Data Minning. Montreal: [s. n.], 1995: 331-336.