Web 安全中的信任管理研究与进展*

徐 锋, 吕 建

(南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093);
(南京大学 计算机软件研究所,江苏 南京 210093)
E-mail: xf@softlab.nju.edu.cn
http://moon.nju.edu.cn

摘要: 信任管理是当前 Web 安全研究的热点.介绍了信任管理思想的出现,给出了信任管理的概念和模型,并概述了几个典型的信任管理系统和信任度评估模型.讨论了当前研究存在的问题以及今后的研究方向.

关 键 词: Web 安全;信任管理
中图法分类号: TP393 文献标识码: A

Internet 的出现,使软件系统的形态发生了根本性的转变.从早期的网络服务到 Web 服务,进而发展到智能 Web 服务,软件系统正从面向封闭的、熟识用户群体和相对静态的形式向开放的、公共可访问的和高度动态的服务模式的转变.这种转变使得 Web 应用系统的安全分析复杂化,同时使许多基于传统软件系统形态的安全技术和手段,尤其是安全授权机制,如访问控制列表(access control list,简称 ACL)、一些传统的公钥证书体系等,不再适用于解决 Web 安全问题.

ACL 一直是各类操作系统中广泛使用的安全机制,采用列表的方式描述用户对系统资源的访问权限.由于其形式简单、易于实现,因而能够被许多传统的分布系统所采用.但正如 M. Blaze 等人所指出的,ACL 存在一些根本性的问题从而无法满足 Web 应用此类新兴的分布系统的安全需求[1]:(1) 用户身份鉴别困难,用户不一定为系统所熟知;(2) 缺乏委托机制,分布的系统管理任务需要委托机制的支持;(3) 表达能力和可扩展性差,无法处理多变的安全条件和个性化的安全需求;(4) 本地信任策略不能跨越管理域,而 Web 应用往往需要跨越多个管理域.虽然有一些改进的方法,如将基于身份标识的公钥系统与 ACL 结合起来使用,但仍然无法从根本上解决所有的问题.传统的基于公钥系统的证书体系,如 X.509,PGP 等,也不能很好地满足 Web 安全的需求.R. Khare 等人对这些证书体系进行了评论[2],指出了层次式证书体系的不足:(1) 认证中心仅担保一般意义上的个体标识,并不去证实个体的能力或赋予其权限;(2) 完全依靠认证中心,弱化了个体的自我信任,而盲目信任大范围内的认证中心,则往往无法解决个体间的利益冲突;(3) 难以集中维护证书撤消列表,证书很可能被滥用.另外,依靠个体进行身份认证和推荐的公钥证书体系,虽然具有很大的灵活性,但是没有集中的信任代理,将使其很难适用于一个较大规模的用户群体.

Web 安全需要新的思想和方法.1996 年,M. Blaze 等人为解决 Internet 网络服务的安全问题首次使用了“信任管理(trust management)”的概念[3],其基本思想是承认开放系统中安全信息的不完整性,系统的安全决策需要依靠可信任第三方提供附加的安全信息.信任管理的意义在于提供了一个适合 Web 应用系统开放、分布和动态特性的安全决策框架.与此同时,A. Adul-Rahman 等学者则从信任的概念出发,对信任内容和信任程度进行划

* 收稿日期: 2002-02-25; 修改日期: 2002-07-02
基金项目: 国家自然科学基金资助项目(60273034);国家高技术研究发展计划资助项目(2001AA113110;2002AA116010);江苏省自然科学基金和高技术资助项目(BG2001012;BK2002203;BK2002409)
作者简介: 徐锋(1975－),男,江苏张家港人,博士生,主要研究领域为分布对象技术,系统安全,电子商务应用;吕建(1960－),男,江苏南京人,博士,教授,博士生导师,主要研究领域为形式化方法,分布对象技术,构件技术.

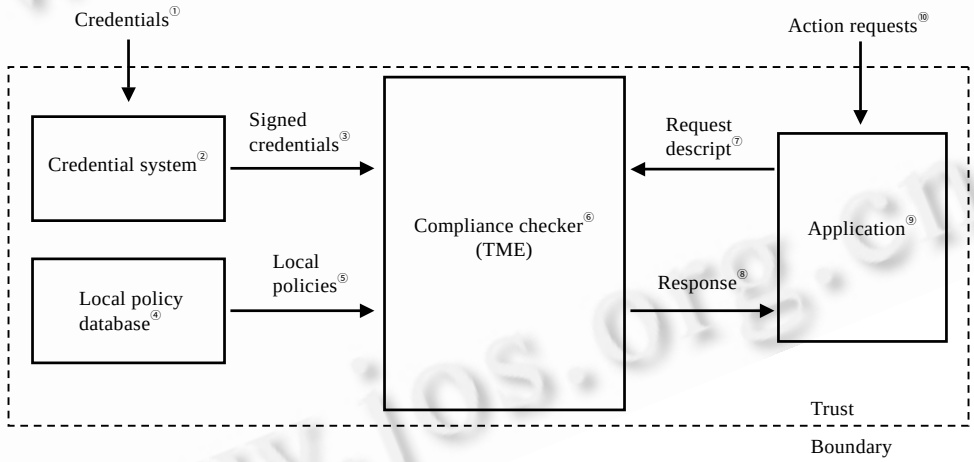
分,并从信任的主观性入手给出信任的数学模型用于信任评估[4~7].

信任管理将传统安全研究中,尤其是安全授权机制研究中隐含的信任概念抽取出来,并以此为中心加以研究,为解决 Web 环境中新的应用形式的安全问题提供了新的思路.信任管理研究可用于安全协议分析,并可结合加密技术等研究成果,指导新的应用系统安全机制的建立.

本文首先给出信任管理的定义和模型,随后详细概述并分析几个有代表性的信任管理系统和信任度评估模型,最后提出当前信任管理研究存在的问题以及今后的研究方向.

1 信任管理的定义和模型

M. Blaze 等人将信任管理定义为采用一种统一的方法描述和解释安全策略(security policy)、安全凭证(security credential)以及用于直接授权关键性安全操作的信任关系(trust relationship)[1].基于该定义,信任管理的内容包括:制定安全策略、获取安全凭证、判断安全凭证集是否满足相关的安全策略等.信任管理要回答的问题可以表述为"安全凭证集 C 是否能够证明请求 r 满足本地策略集 P".在一个典型的 Web 服务访问授权中,服务方的安全策略形成了本地权威的根源,服务方既可使用安全策略对特定的服务请求进行直接授权,也可将这种授权委托给可信任第三方.可信任第三方则根据其具有的领域专业知识或与潜在的服务请求者之间的关系判断委托请求,并以签发安全凭证的形式返回委托请求方.最后,服务方判断收集的安全凭证是否满足本地安全策略,并作出相应的安全决策.为了使信任管理能够独立于特定的应用,M.Blaze 等人还提出了一个基于信任管理引擎(trust management engine,简称 TME)的信任管理模型,如图 1 所示.TME 是整个信任管理模型的核心,体现了通用的、应用独立的一致性证明验证算法,根据输入的三元组(r,C,P),输出策略是否被满足的判断结果.几个典型信任管理系统[3,8,9]均以该模型为基础进行设计并加以实现.



①凭证,②凭证系统,③签名凭证,④本地策略库,⑤本地策略,⑥一致性验证器(信任管理引擎),⑦请求描述,⑧响应,⑨应用系统,⑩动作请求.

Fig.1 Trust management model

图 1 信任管理模型

D. Povey 在 M. Blaze 定义的基础上,结合 A. Adul-Rahman 等人提出的主观信任模型思想[4~7],给出了一个更具一般性的信任管理定义,即信任管理是信任意向(trusting intention)的获取、评估和实施[10].授权委托和安全凭证实际上是一种信任意向的具体表现,而主观信任模型则主要从信任的定义出发,使用数学的方法来描述信任意向的获取和评估.主观信任模型认为,信任是主体对客体特定行为的主观可能性预期,取决于经验并随着客体行为的结果变化而不断修正[11].在主观信任模型中,实体之间的信任关系分为直接信任关系和推荐信任关系,分别用于描述主体与客体、主体与客体经验推荐者之间的信任关系.也就是说,主体对客体的经验既可以直接获得,又可以通过推荐者获得,而推荐者提供的经验同样可以通过其他推荐者获得,直接信任关系和推荐信任关系形成了一条从主体到客体的信任链,而主体对客体行为的主观预期则取决于这些直接的和间接的经验.信任

模型所关注的内容主要有信任表述、信任度量和信任度评估.信任度评估是整个信任模型的核心,因此信任模型也称信任度评估模型.信任度评估与安全策略的实施相结合同样可以构成一个一般意义上的信任管理系统.P. Herrmann 等人提出了一个“信任适应的安全策略实施(trust-adapted enforcement of security policy)”的概念,并在这方面做了一些初步的研究[12].

2 信任管理系统

从信任管理模型可以看出,信任管理引擎是信任管理系统的核心.而设计信任管理引擎需要涉及以下几个主要问题[1]:(1) 描述和表达安全策略和安全凭证;(2) 设计策略一致性证明验证算法;(3) 划分信任管理引擎和应用系统之间的职能.当前几个典型的信任管理系统 PolicyMaker[3],KeyNote[8]和 REFEREE[9]在设计和实现信任管理引擎时采用了不同的方法来处理上述问题.

2.1 PolicyMaker

PolicyMaker 是 M. Blaze 等人依据他们所提出的信任管理思想较早实现的信任管理系统.PolicyMaker 为网络服务安全授权提供了一个完整而直接的解决方法,取代了传统的认证和访问控制相结合的做法,并且给出了一个独立于特定应用的一致性证明验证算法,用于服务请求、安全凭证和安全策略的匹配.

PolicyMaker 采用一种完全可编程的机制来描述安全策略和安全凭证,所有的安全策略和安全凭证均可归结为断言.每个断言可表达为一个(f,s)对,其中 s 表示权威源(source of authority),f 则是一段用于描述实际授权内容或委托授权内容的程序.在一个安全策略断言中,s 被赋予关键字 POLICY.策略断言是信任管理引擎必不可少的输入参数,描述了应用系统判断请求是否可接受的最终权威根源.而在一个安全凭证断言中,s 则被赋予该安全凭证签发者的公钥.在采纳某个安全凭证时,公钥用于验证该安全凭证的可靠性.PolicyMaker 没有对书写断言内容 f 的程序语言作特别的要求,其原则是只要能被本地应用环境解释的编程语言均可用于书写断言.在其早期的试验性工作中,M. Blaze 等人专门开发了一种名为 AWK 的程序语言用于描述断言内容,该语言的模式匹配结构较适合描述授权信息.

由于 PolicyMaker 没有指明特定的断言描述语言,因此其策略一致性证明验证算法必须独立于特定的断言描述语言.PolicyMaker 进行一致性证明验证的一般步骤描述如下:首先建立一个仅包含请求字符串 r 的黑板.随后,调用断言.同一断言可以根据需要调用多次.另外,断言由本地运行环境解释.当断言(f_i,s_i)运行时,先读取黑板中的内容并根据内容加入一条或多条接受记录(i,s_i,R_{ij}),但不能够删除其他断言已写入黑板的接受记录.其中 R_{ij} 表示一个被权威源 S_i 所证明的特定应用操作,可以是一个输入请求 r,也可以是一些用于断言间交互的操作.算法本身不需要理解和处理 R_{ij},面向特定应用的断言程序 f_i 处理 R_{ij}.最终,当所有断言调用完毕后,若黑板中存在一条能证明请求 r 的接受记录,则一致性证明验证成功.但实际的验证算法还需要解决诸如断言的调用顺序、断言的调用次数和丢弃产生冲突的断言等一系列问题.为此,M. Blaze 等人用数学的方法精确地描述了一致性验证(proof of compliance,简称 PoC)问题[13],并证明一般意义下的 PoC 问题是不可判定的,但一些限定的 PoC 问题存在多项式时间算法.PolicyMaker 实现了一个解决 LBMA PoC 问题的一致性验证证明算法.该算法只能处理满足单调性的策略断言,限制了一些策略的使用,如否定安全凭证(negative credential)等.另外,该算法还要求断言程序 f 的时间复杂性不能大于 $O(n^K)$.

PolicyMaker 是一个实验性质的信任管理系统,其功能相对简单,不提供安全凭证的收集和验证的功能.应用系统必须负责收集并保证足够的安全凭证用于验证相关的操作请求,还需根据安全凭证的公钥信息验证其可靠性,而 PolicyMaker 仅根据应用系统输入的操作请求、安全策略集和安全凭证集来完成最后的一致性证明验证工作.这种信任管理引擎与应用系统的功能划分加重了应用系统的负担,而且可能会因为安全凭证收集不充分而导致一致性证明验证的失败.但应用系统负责安全凭证的可靠性验证,使其在选择签名算法时具有一定的灵活性.

2.2 KeyNote

KeyNote 是 M. Blaze 等人实现的第 2 个信任管理系统.不同于 PolicyMaker,KeyNote 在设计之初就希望能

够促进信任管理系统的标准化并使其易于集成到应用系统中.为此,KeyNote 在系统的设计和实现上与 PolicyMaker 存在着很大的差别.目前,KeyNote 已在 Ipsec 协议[14]、网上交易的离线支付[15]等方面进行了一些应用研究.

考虑到标准化和易读性,KeyNote 采用一种类似于电子邮件信头的格式来描述安全策略和安全凭证断言,如下例所示:

KeyNote-version: 1
Authorizer: rsa-pkcs1-hex: “1023abcd”
Licensees: dsa-hex: “986512a1” || rsa-pkcs1-hex: “19abcd02”
Comment: Authorizer delegates read access to editor of the licensees
Conditions: ($file==“/etc/passwd” && $access==“read”)→{return “ok”}
Signatures: rsa-md5-pkcs1-hex: “f00f5673”

其中 Authorizer 字段等同于 PolicyMaker 中的断言权威源 *s*,以实体的公钥标识.Licensees 字段用于显式地指定被授权或被委以授权的实体,同样以其公钥标识,并且多个实体公钥之间可以使用逻辑运算符,合取、析取和阈等进行连接.Comment 字段用于断言的注释.Conditions 字段描述断言判断程序,用于测试 KeyNote 应用系统提供的操作环境变量,其中包含了请求相关和信任判断必须的信息.测试使用的运算操作主要有字符串匹配、数值运算、数值比较和模式匹配等.KeyNote 仅接受其提供的这种简单的断言描述语言所描述的断言.关于断言及其语法的详细描述参见文献[16].

KeyNote 的一致性证明验证算法是一种深度优先算法.其主要思想是采用递归的方式试图查找到至少一条能够满足请求的策略断言.所谓满足一个断言,即该断言的 Condition 字段和 Licensees 字段同时得到满足.KeyNote 中断言程序运行时,也能根据断言的满足情况生成类似于 PolicyMaker 的接受记录,但该记录仅被 KeyNote 的验证模块内部使用,对其他断言程序不可见.最终,当由请求、断言和断言间的证明关系所形成的图被构造出来时,该请求被证明.相对于 Policymaker 而言,KeyNote 一致性验证算法对输入的断言要求更严格,因此,KeyNote 一致性验证算法实际上解决的 PoC 问题仅是 PolicyMaker 的一个子集.KeyNote 同样不能处理非单调性的断言.

KeyNote 提供一种专门的语言以描述安全策略和安全凭证断言,并且负责安全凭证的可靠性验证.这一方面减轻了应用系统的负担,使 KeyNote 更容易与应用系统集成;另一方面则有利于安全策略和安全凭证描述格式的标准化,使应用系统能够更有效地传播、获取以及使用安全策略和安全凭证.

2.3 REFEREE

REFEREE 是 Y.-H. Chu 等人为解决 Web 浏览安全问题而开发的信任管理系统.虽然其设计目标比较单一,但该系统可以较完整地实现信任管理模型所列出的各要素.

REFEREE 采用了与 PolicyMaker 类似的完全可编程的方式描述安全策略和安全凭证.在 REFEREE 系统中,安全策略和安全凭证均被表达为一段程序,但程序必须采用 REFEREE 约定的格式来描述,如下例所示:

```
(invoke “load-label” STATEMENT-LIST URL “http://www.musac.org/” (EMBEDDED))
(false-if-unknown
        (match
           ((“load-label”*)
            (*((version “PICS-1.1”)*
                (service “http://www.musac.org/”)*
                (ratings    (RESTRICT<s2)))))
STATEMENT-LIST))
```

程序的输入通常是一个声明列表 STATEMENT-LIST,用于定义当前策略或凭证的验证上下文,程序也可以接受一些附加参数.程序的输出包括一个判断结果(接受、拒绝或未知)和一个声明列表.

REFEREE 的一致性证明验证过程比较复杂,整个验证过程由安全策略或安全凭证程序之间的调用完成,程序甚至能根据具体需求自主地收集、验证和调用相关的安全凭证.另外,REFEREE 能够验证非单调的安全策略和安全凭证,即能够处理一些否定安全凭证.REFEREE 灵活的一致性证明验证机制一方面使其具有较强的处理能力,另一方面也导致其实现代价较高.而允许安全策略和安全凭证程序间的自主调用则存在较大的安全隐患.另外,必须看到 REFEREE 的验证结果可能会出现未知的情况.

REFEREE 能够在一致性证明验证时自动收集并验证安全凭证的可靠性,应用系统仅需给出初始的安全策略、安全凭证和验证内容以及一些必要的验证上下文信息.这一点有利于该信任管理系统的使用.

3 信任度评估模型

M. Blaze 等人提出并实现的信任管理系统的本质是使用一种精确的、理性的方式来描述和处理复杂的信任关系.但在信任管理思想提出之前和之后,都有一些学者,如 D. Gambetta, A. Adul-Rahman 等人,认为信任是非理性的[4,11],是一种经验的体现,不仅要有具体的内容,还应有程度的划分,并提出了一些基于此观点的信任度评估模型.信任度评估模型主要涉及以下问题:(1) 信任的表述和度量;(2) 由经验推荐所引起的信任度推导和综合计算.几个有代表性的信任度评估模型在上述内容的处理上存在差异.

3.1 Beth信任度评估模型

Beth 信任度评估模型引入了经验的概念来表述和度量信任关系,并给出了由经验推荐所引出的信任度推导和综合计算公式.

在 Beth 信任度评估模型中,经验被定义为对某个实体完成某项任务的情况记录,对应于任务的成败,经验被分为肯定经验和否定经验.若实体任务成功则对其的肯定经验记数增加,若实体任务失败则否定经验记数增加.模型中的经验可以由推荐获得,而推荐经验的可性度问题同样是信任问题.为此,模型将信任被分为直接信任和推荐信任.直接信任定义为“若 P 对 Q 的所有(包括直接的或由推荐获得的)经验均为肯定经验,则 P 对 Q 存在直接信任关系”.当 Q 被信任时,Q 能成功完成任务的概率被用于评价这种信任关系,而概率的计算则取决于 P 对 Q 的肯定经验记录.Beth 采用以下公式描述直接信任度与肯定经验记录的关系:

$$v_z(p)=1-\alpha^p,$$

其中 p 是 P 所获得的关于 Q 肯定经验数,α 则是对 Q 成功完成一次任务的可能性期望.该公式基于 Q 完成一次任务的可能性在[0,1]上均匀分布这一假设.推荐信任定义为“若 P 愿意接受 Q 提供的关于目标实体的经验,则 P 对 Q 存在推荐经验关系”.Beth 采用肯定经验与否定经验相结合的方法描述推荐信任度.推荐信任度与经验记录的关系采用如下公式描述:

$$v_r(p,n)=\begin{cases}1-\alpha^{p-n}, & \text{if } p>n\\ 0, & \text{else}\end{cases},$$

其中 p,n 分别是 P 所获得的关于 Q 的肯定经验和否定经验数.

在 Beth 信任度评估模型中,经验可以通过推荐获得.而对于同一个信任关系,多个不同的经验推荐者可能形成多条不同的推荐路径.这就需要有一个计算方法能够推导并综合所有推荐路径的经验信息,以获得一致的信任度.Beth 分别对直接信任和推荐信任进行了讨论,并给出了相应的信任度推导和综合计算公式.假设 A 对 B 的推荐信任度为 V_1,B 对 C 的直接信任度为 V_2,B 对 D 的推荐信任度为 V_3,则 A 对 C 的直接信任度推导公式表述为

$$V_1 \odot V_2 = 1-(1-V_2)^{V_1}.$$

A 对 D 的推荐信任度可以简单地表述为 $V_1 \cdot V_3$.Beth 模型还给出了推荐信任度综合计算公式:

$$V_{\text{com}}=\frac{1}{n}\sum_{i=1}^{n}V_i.$$

其中 V_i 是由单个推荐路径而推导出的信任度,综合推荐信任度 V_{com} 是这些单个信任度的简单算术平均.设 $P_i(i=1,...,m)$ 是推荐路径上各不相同的最终推荐实体,$V_{i,*}$ 表示其最终推荐实体为 P_i 的各条推荐路径的信任度,

则直接信任度综合计算公式表述为

$$V_{\text{com}} = 1 - \prod_{i=1}^{m} n_i \sqrt{\prod_{j=1}^{n_i} \left(1 - V_{i,j}\right)}.$$

该公式考虑了同一个经验推荐者出现在不同推荐路径上的情况.相同的经验信息经不同的路径被多次传递,产生不同的推导结果,该公式采用取推导值平均的方法得到一个惟一值.

Beth 模型对直接信任的定义比较严格,仅采用肯定经验对信任关系进行度量.另外,其信任度综合计算采用简单的算术平均,无法很好地消除恶意推荐所带来的影响.

3.2 Jøsang信任度评估模型

Jøsang 等人引入了事实空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系,并提供了一套主观逻辑(subjective logic)运算子用于信任度的推导和综合计算[17~20].

事实空间由一系列实体产生的可观察到的事件组成.实体产生的事件被简单地划分为肯定事件(positive event)和否定事件(negative event).Jøsang 基于 Beta 分布函数描述二项事件(binary event)后验概率的思想,给出了一个由观察到的肯定事件数和否定事件数决定的概率确定性密度函数 pcdf,并以此来计算实体产生某个事件的概率的可信度.设概率变量为 θ,r 和 s 分别表示观测到的实体所产生的肯定事件和否定事件数,则 pcdf 公式表述为

$$\varphi(\theta \mid r,s) = \frac{\Gamma(r+s+2)}{\Gamma(r+1)\Gamma(s+1)} \theta^r (1-\theta)^s,\ 0 \le \theta \le 1, r \ge 0, s \ge 0.$$

观念空间则由一系列对陈述的主观信任评估组成.主观信任度由三元组 $\omega = \{b,d,u\}$ 描述.该三元组满足:

$$b + d + u = 1,\quad \{b,d,u\} \in [0,1]^3,$$

其中 b,d,u 分别描述对陈述的信任程度、不信任程度和不确定程度.Jøsang 使用如下公式将 ω 定义为事实空间中肯定事件数 r 和否定事件数 s 的函数:

$$\begin{cases} b = \dfrac{r}{r+s+1} \\ d = \dfrac{s}{r+s+1} \\ u = \dfrac{1}{r+s+1} \end{cases},$$

并认为 ω 与 pcdf 在主观信任度的表达上是等价的,也即可以通过事实空间的统计事件来描述主观信任度.

Jøsang 信任度评估模型提供了一套主观逻辑算子,用于信任度之间的运算.其主要的算子有合并(cojunction)、合意(consensus)和推荐(recommendation).其中合并用于不同信任内容的信任度综合计算.合意根据参与运算的观念(信任度)之间的关系分为独立观念间的合意、依赖观念间的合意和部分依赖观念间的合意 3 类.所谓观念依赖是指观念是否部分或全部由观察相同的事件所形成.合意主要用于对多个相同信任内容的信任度综合计算.推荐主要用于信任度的推导计算.详细的主观逻辑算子的描述参见文献[18].

与 Beth 模型相比,Jøsang 模型对信任的定义较宽松,同时使用了事实空间中的肯定事件和否定事件对信任关系进行度量.模型没有明确区分直接信任和推荐信任,但提供了推荐算子用于信任度的推导.另外,其信任度使用三元组来表示,而不是 Beth 模型中的单一数值.该模型同样无法有效地消除恶意推荐带来的影响.

4 当前研究存在的问题

目前,以 Web 服务为代表的软件服务及软件服务协同已成为一种新兴的 Web 应用形态.Web 应用体现为一个由多个软件服务组成的动态协同系统,而服务本身也可以由其他服务动态组合而成.Web 安全具有了一些新的特点和要求,主要表现在:(1) 安全分析主体的复杂化,Web 应用系统安全分析的主体除了用户和系统所有者以外,还应包括服务提供者、服务营运者等;(2) 安全信息的不完整性,服务的本质在于开放,因此不能期望服务使用方与服务提供方之间相互熟知,而且完全掌握对方的安全相关信息;(3) 安全度量的相对化,Web 环境的开

放、动态特性产生了更多影响系统安全的不确定因素,无法使用绝对的、精确的标准来衡量系统的安全性;(4) 安全需求的个性化,不同的应用系统和服务对安全的需求不同,即使是组成同一应用系统的服务也具有不同的安全需求;(5) 安全措施实施的自适性,Web 环境是高度动态和多变的,安全措施的实施必须能够实时地适应这种变化.

信任管理提供了一个适宜解决新的 Web 应用形态下的安全问题的框架,但当前几个已实现的信任管理系统还存在着一些不足:(1) 安全分析主体的单一,仅考虑服务方的安全保护,没有考虑服务调用方的安全问题;(2) 安全度量的绝对化,采用策略一致性证明验证的方法进行安全度量和决策,该方法过于精确,不能很好地适应 Web 安全环境的多变性和不确定性;(3) 无法实时地满足动态的安全环境的变化,安全策略验证的能力和效率有限,并且大部分信任管理系统在策略一致性证明验证前必须收集足够的安全凭证.另外,安全策略的制定过程较为繁复,也阻碍了这些信任管理系统的应用.

一些主观信任模型提出的信任度量和评估,其实质是采用一种相对的方法对安全信息进行度量和评估,能够较好地反映出 Web 安全环境的多变性和不确定性,并且该方法较适合信任信息收集、评估的自动化实现.信任度量和评估与实际的安全策略的实施相结合将是信任管理系统实现的新途径.但必须看到,当前几个代表性的信任度评估模型还存在一些问题:(1) 信任的表述和度量的合理性有待于进一步解释,现有的模型倾向于采用事件概率的方式来表述和度量信任关系,都是基于一定的概率分布假设;(2) 不能很好地解决恶意推荐对信任度评估的影响,现有的模型大多采用求简单算术平均的方法综合多个不同推荐路径的信任度;(3) 当前的信任度评估模型缺少灵活的机制,如参数设置,以反映不同实体进行信任评估时所具有的个性特点.

5 结束语

本文介绍了信任管理思想的出现,并就信任管理模型和几个典型的信任管理系统实现进行了详细的讨论和分析,另外还介绍和分析了与当前信任管理研究相关的几个具有代表性的主观信任度评估模型.随着 Web 应用的不断发展,Web 安全将具有更多的内涵.同时,Web 动态性、开放性的增强将给安全问题带来更多的不确定性和复杂性.基于策略的信任管理系统还存在着诸多问题,如一致性证明验证算法能力有限、策略制定过程每繁琐、难以处理不确定的安全信息等等.而主观信任度评估与安全策略实施相结合的信任管理思想刚刚被提出来,有待于进一步的研究和实现.

References:

[1] Blaze, M., Feigenbaum, J., Ioannidis, J., *et al*. The role of trust management in distributed systems security. In: Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999. 185~210.

[2] Khare, R., Rifkin, A. Trust management on World Wide Web. World Wide Web Journal, 1997,2(3):77~112.

[3] Blaze, M., Feigenbaum, J., Lacy, J. Decentralized trust management. In: Dale, J., Dinolt, G., eds. Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996. 164~173.

[4] Abdul-Rahman, A., Hailes, S. A distributed trust model. In: Proceedings of the 1997 New Security Paradigms Workshop. Cumbria, UK: ACM Press, 1998. 48~60. http://www.ib.hu-berlin.de/~kuhlen/VERT01/abdul-rahman-trust-model1997.pdf.

[5] Abdul-Rahman, A., Hailes, S. Using recommendations for managing trust in distributed systems. In: Proceedings of the IEEE Malaysia International Conference on Communication'97 (MICC'97). Kuala Lumpur: IEEE Press, 1997. http://citeseer.nj.nec.com/360414.html.

[6] Yahalom, R., Klein, B., Beth, T. Trust relationships in secure systems——a distributed authentication perspective. In: Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy. IEEE Press, 1993. 50~164. http://isbn.nu/0818633700.

[7] Beth, T., Borcherding, M., Klein, B. Valuation of trust in open network. In: Gollmann, D., ed. Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3~18.

[8] Blaze, M., Feigenbaum, J., Keromytis, A.D. Keynote: trust management for public-key infrastructures. In: Christianson, B., Crispo, B., William, S., *et al*., eds. Cambridge 1998 Security Protocols International Workshop. Berlin: Springer-Verglag, 1999. 59~63.

[9] Chu, Y.-H., Feigenbaum, J., LaMacchia, B., *et al*. REFEREE: trust management for Web applications. World Wide Web Journal, 1997,2(2):127~139.

[10] Povey, D. Developing electronic trust policies using a risk management model. In: Proceedings of the 1999 CQRE Congress. 1999. 1~16. http://security.dstc.edu.au/staff/povey/papers/CQRE/123.pdf.

[11] Gambetta, D. Can we trust trust? In: Gambetta, D., ed. Trust: Making and Breaking Cooperative Relations. Basil Blackwell: Oxford Press, 1990. 213~237.

[12] Herrmann, P., Krumm, H. Trust-Adapted enforcement of security policies in distributed component-structured applications. In: Proceedings of the 6th IEEE Symposium on Computers and Communications. Hammamet: IEEE Computer Society Press, 2001. 2~8. http://www.computer.org/proceedings/iscc/1177/11770002abs.htm.

[13] Blaze, M., Feigenbaum, J., Strauss, M. Compliance Checking in the PolicyMaker Trust Management System. In: Hirschfeld, R., ed. Proceedings of the Financial Cryptography'98. Lecture Notes in Computer Science 1465, Berlin: Springer-Verlag, 1998. 254~274.

[14] Blaze, M., Ioannidis, J., Keromytis, A. Trust management for IPSec. In: Proceedings of the Internet Society Symposium on Network and Distributed Systems Security (SNDSS 2001). 2001. 139~151. http://www.cis.upenn.edu/~strongman/papers/tmipsec.pdf.

[15] Blaze, M., Ioannidis, J., Keromytis, A. Offline Micropayments without Trusted Hardware. In: Syverson, F. ed. Financial Cryptography 2001. Lecture Notes in Computer Science 2339, Berlin: Springer Verlag, 2002.

[16] Blaze, M., Feigenbaum, J., Ioannidis, J., *et al*. The KeyNote trust management system version 2. Internet RFC 2704, 1999.

[17] Jøsang, A. The right type of trust for distributed systems. In: Meadows, C., ed. Proceedings of the 1996 New Security Paradigms Workshop. Lake Arrowhead, CA: ACM Press, 1996.

[18] Jøsang, A. A model for trust in security systems. In: Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. 1997. http://security.dstc.edu.au/staff/ajosang/papers.html.

[19] Jøsang, A., Knapskog, S.J. A metric for trusted systems. Global IT Security. Wien: Austrian Computer Society, 1998. 541~549.

[20] Jøsang, A. A Subjective Metric of Authentication. In: Quisquater, J., ed. Proceedings of the ESORICS'98. Louvain-la-Neuve.: Springer Verlag, 1998. 329~344.

Research and Development of Trust Management in Web Security*

XU Feng, LÜ Jian

(*State Key Laboratory for Novel Software Technology*, *Nanjing University*, *Nanjing* 210093, *China*);

(*Institute of Computer Software*, *Nanjing University*, *Nanjing* 210093, *China*)

E-mail: xf@softlab.nju.edu.cn

http://moon.nju.edu.cn

Abstract: Trust management is a hot topic of Web security research in recent years. In this paper, the emerging of trust management is presented. Its concepts and models are described in detail, and several typical trust management systems and trust valuation models are introduced. The existing problems of current works and future research direction are discussed.

Key words: Web security; trust management

* Received February 25, 2002; accepted July 2, 2002

Supported by the National Natural Science Foundation of China under Grant No.60273034; the National High-Tech Research and Development Plan of China under Grant Nos.2001AA113110, 2002AA116010; the Foundation of Nature Science and Hi-Technology of Jiangsu Province of China under Grant Nos.BG2001012, BK2002203, BK2002409