基于 XML 的安全管理平台中信任管理机制的研究和实现*)

彭 杰 郭山清 茅 兵 谢 立

(南京大学软件新技术国家重点实验室 南京 210093) (南京大学计算机科学与技术系 南京 210093)

摘 要 本文分析了当今安全管理系统暴露出的诸多问题,并且在基于 XML 的安全管理平台中引入了信任管理机制。在传统的信任模型中,信任主体是单一的,这不能满足提高基于 XML 的安全管理信任的要求。为了解决这个问题,对传统的信任模型进行了一些必要的改进。首先,双向的信任被提出来,用以解决服务器与客户端的相互信任问题;其次,增加了一个局域的信任库,以提高管理员的整体分析能力和基于历史声誉的信任度评估能力。

关键词 安全管理,信任管理

The Research and Implementation of Trust Management Mechanism in the XML-Based Security Management Platform

PENG Jie GUO Shan-Qing MAO Bing XIE Li

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

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract In this paper, we analyze the problems exposed by the current security management systems, and introduce the trust mechanism to XML-based security management platform. In the traditional trust model, the trust subject is unitary, which can not meet the requirements raised by the XML-based security management to trust. In order to solve this problem, some necessary improvements are made to the traditional trust model. First, the bidirectional trust is proposed, resolving the mutual trust problem of the server and client. Second, a local trust library is added to enhance both the administrator's global analysis and the assessment of reputation-based trust degree.

Keywords Security management, Trust management

1 引言

随着 Internet 的飞速发展,越来越多的安全设备被应用到企业、政府和学校的网络中,如何协调这些安全设备,并通过对它们进行有效的管理为用户提供一个安全、可信的网络环境成为一个重要的研究课题。

安全管理通过适当的识别企业的信息资产,评估信息资产的价值,制定、实施安全策略、安全措施来保证企业信息资产的完整性、机密性和可用性。目前主要的安全管理系统有 Cisco 的 Cisco Secure Policy Manager(安全策略管理器)[1]和 IBM 的 Tivoli[2]。它们都在一定程度上对网络中的安全设备进行统一的配置和管理,但它们自身也存在一些缺陷,即现有的安全管理系统没有提供一整套有效的安全机制来对其自身的安全进行管理,因此可能被黑客利用而进行冒名,欺骗,DOS 等攻击,进而窃取机密信息,甚至破坏整个网络正常的运营状况,给公司或企业造成巨大损失。

对于上述问题,信任管理提供了一个有效的解决方案。信任管理通过采用第三方签发的安全凭证和本地安全策略,验证请求是否许可。但是传统的基于策略的信任管理模型仍存在如下不足:1) 信任主体单一,仅考虑服务调用方到服务方的信任验证,没有考虑服务方返回结果的信任验证问题;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[6]。

在分析了上述安全管理系统以及传统的基于策略的信任管理模型的不足的基础上,针对具体的安全管理应用,我们设计并开发了基于 XML 的安全管理平台(XBSP),该安全管理平台集成了 WEB,XML 以及相关技术,对底层的防火墙,IDS 等安全设备提供了一致的安全管理界面和操作集。XBSP 针对现有安全管理系统中存在的对自身安全管理缺乏等问题,引入了信任管理的机制,并在一定程度上对其进行扩展,弥补了传统信任模型的不足,有效地防止了上述安全隐患。

本文首先介绍了相关领域的工作,随后详细介绍了一种基于 XML 的安全管理平台及信任管理机制的研究和设计,最后总结本文工作并展望下一步的研究方向。

2 相关工作

2.1 安全管理

目前主要的安全管理系统有 Cisco 的 Cisco Secure Policy Manager(安全策略管理器)[1]和 IBM 的 Tivoli[2]。其中 Cisco Secure Policy Manager(CSPM)可以制定、分发、实施和审计整个网络的安全策略;自动地将网络策略转换成相应的 Cisco 防火墙和 VPN 路由器的命令行配置;验证它所管理的网络拓扑、所制定的安全策略和所生成的配置的完整性和配置的正确性。但其仅限于 Cisco PIX 防火墙和 IP 安全(IPSec)虚拟专用网(VPN)路由器,且不能对网络中的实体进行信任确立,容易被黑客利用而进行欺骗攻击;Tivoli 是构建企业安全管理的平台软件,它属于 3A(认证、授权和管理)软件,而非网络安全软件,如防火墙、防病毒、入侵侦测软件等。同样,Tivoli 也没有提供信任管理的功能。

2.2 信任管理

信任管理(trust management)作为一个整体概念是由

*)本文得到国家"863"高技术(NO:2003AA144010)经费资助。彭 杰 硕士生,研究方向:信息安全。郭山清 博士生,研究方向:分布式系统,网络安全。茅 兵 教授,博导,研究方向:系统安全。谢 立 教授,博导,研究方向:分布式计算,先进操作系统。

M. Blaze 等第一次提出的。信任管理被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)。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描述为"凭证集 C(credential) 是否能够证明请求 r(request)遵守本地安全策略 P (policy)"[3,5]。

信任管理将安全策略、凭证、访问控制和授权的概念统一在一个信任框架里面,给当今日益庞大、分布式的网络应用提供了一种很好的安全管理机制。信任管理问题包括以下几个方面[3]:(1)明确地定义安全策略和安全凭证;(2)确定特定的凭证集是否满足相关的策略;(3)信任委托。

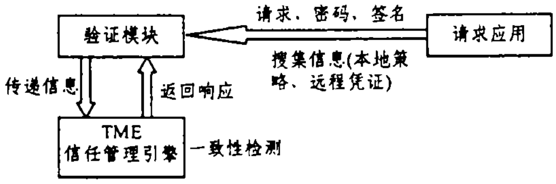

图 1 应用程序与 TME 之间的交互

在一个集成了信任管理的应用程序中,每个收到请求的实体都必须与一个作为授权源的本地策略相关联,该实体的策略可能直接授权某个公钥执行某种操作,也可能将这个责任委托给它所信赖的凭证发行者。信任管理引擎(TME)是一个独立的系统组件,它以(r,C,P)作为输入,回答上面提到的问题。图 1 说明了一个应用与一个信任管理系统交互的例子[7]:

由 M. Blaze 等开发的 PolicyMaker 是第一个信任管理系统[3,4],随后他们又开发了 KeyNote 信任管理系统[8,9]。PolicyMaker 侧重于研究而 KeyNote 则更偏向于实用,它们有相同的基本语义结构。其他的信任管理系统和模型有 Yang-Hua Chu 等开发的 REFEREE[10],IBM 的信任确立框架[11,12]等。

3 基于 XML 的安管平台中的信任管理

基于 XML 的安全管理平台(XBSP)主要对基于 SNMP 协议的不同类别的安全产品提供统一集中的管理,具体实现对防火墙和 IDS 等安全产品的管理。

在 XBSP 中,针对现有安全管理平台没有对自身安全提供管理功能的缺陷,我们引入了信任管理的机制;针对传统的信任模型在信任主体单一和安全度量绝对化方面的不足进行了扩充,加入了本地信任库和双向信任的功能。下面,我们将从系统总体结构、数据流分析和系统中信任管理元素的定义和设计三方面对 XBSP 中的信任管理机制和实现进行阐述。

3.1 系统总体结构

XBSP 主要由 7 部分组成,其总体结构如图 2 所示。各部分功能简述如下:

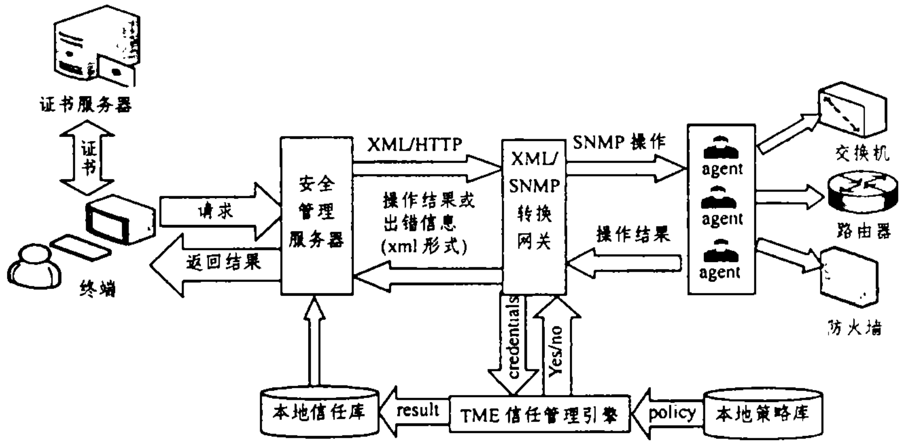

图 2 XBSP 总体结构

(1)证书服务器:为整个平台统一提供证书;(2)安全管理服务器:接收安全管理员的输入,根据安全管理员所选择的凭证,所请求的操作生成相应的 XML 文档,提交给 XML/SNMP 转换网关;(3)XML/SNMP 转换网关:解析从安管服务器接收的 XML 文档,分离出其中的凭证,操作部分,将其提交给 TME(信任管理引擎),根据 TME 的返回执行相关操作;(4)TME(信任管理引擎):根据 XML/SNMP 转换网关发送的凭证、本地策略,判断是否允许相应的操作,并将判断结果写入本地信任库,便于日后分析;(5)本地策略库:制定对系统中资源的访问规则,说明"谁可以对何种资源进行何种操作";(6)本地信任库:存储每次的一致性检测结果,将结果以 XML 文档的形式发送给安管服务器以便于管理员对系统状态,可能存在的薄弱点进行全局分析;(7)底层 agent 及被管设备:系统中的安全产品,比如防火墙,IDS 等。

与传统的信任管理模型相比,XBSP 加入了本地信任库用来存储 TME 每次的判断结果,本地信任库有两个主要功能:首先它将信任库中的信任信息以 XML 文档的形式发送给安管服务器,可以很方便地显示给管理员或终端用户;其次为以后信任度评估模型的研究提供了依据,下一步会进行基于历史声誉(reputation-based)的信任度评估方面的研究,本地信任库中记录了系统中各实体相关的信任信息,可以作为信任度评估的一个重要依据。

与传统的基于策略的信任模型不同的是,针对安全管理这样的具体应用,我们加入了双向信任的功能,即不仅安全管理员对被管设备进行操作要进行信任验证,被管设备向安管服务器返回的数据也要经过信任验证。这样的双向信任是有必要的,考虑如下欺骗场景:管理员发送请求,要求获取某防火墙的状态,而该防火墙已被某黑客攻陷,该黑客伪造了防火墙工作正常的消息并将该消息发送给安全管理员,给管理员造成网络正常的假相。

3.2 数据流分析

在 XBSP 中存在三种数据流:控制数据流,设备信息数据

流和一致性判断结果数据流，对这三种主要数据流的分析如下：

(1)*控制数据流* a)安全管理员登录安全管理服务器，进行初级身份认证(username/password)；b)进入安全管理界面，选择所使用的证书以及对何种安全设备执行何种操作；c)安管服务器根据安全管理员所选择的证书和操作生成相应的XML文档，并提交给XML/SNMP转换网关；d) XML/SNMP转换网关对该XML文档进行解析，提取出所需要的信息(凭证，操作等)，并将这些信息提交给TME；e)TME根据XML/SNMP转换网关提供的凭证，以及本地策略库中的策略，判断安管员所请求的操作是否遵守本地策略，并将结果返回给XML/SNMP转换网关；f) 根据TME返回的结果，XML/SNMP转换网关执行如下操作：如果结果为允许执行所请求操作，则XML/SNMP转换网关将该操作转换为对应的SNMP操作，并发送给底层对应设备的agent；否则，若拒绝该操作，由XML/SNMP转换网关生成相应的出错报告返回给安管服务器；g)底层agent执行请求的操作。

(2)*设备信息数据流* a) Agent将执行结果和agent的证书一起返回给XML/SNMP转换网关；b) XML/SNMP转换网关将该证书提交给TME，以判断该结果是否值得信任；c) TME根据对该证书进行信任验证，并将结果返回给XML/SNMP转换网关；d) 若TME返回该操作结果可信，则XML/SNMP转换网关将该操作结果封装成XML文档，并返回给安管服务器；否则，若TME返回该操作结果不可信，则生成该操作不成功的报告并返回给安管服务器；e) 安管服务器将返回数据显示给用户。

(3)*一致性判断结果数据流* a) 同(1)的a)，b)，c)，d)步骤或(2)的a)，b)步骤；b) TME将判断结果写入本地信任库；c) 安管服务器查询本地信任库，并将结果显示给终端用户。

安全管理服务器与XML/SNMP转换网关之间的通信基于HTTP协议，XML/SNMP转换网关与设备agent之间的通信则基于SNMP协议。控制数据流和设备信息数据流均通过SSL加密，保证了底层通信的安全性。

3.3 信任管理元素的定义和表示

一个信任管理系统典型地由5个基本部分组成[9]：1) 描述行为(action)的语言；2) 标识实体(principal)的机制；3) 说明策略(policy)的语言；4) 说明凭证(credential)的语言；5) 一致性检测算法(compliance checking)。

XBSP中策略和凭证都是用XML文档来表述的。XBSP中主要存在三类用户：安全管理员，数据库管理员和一般用户。安全管理员对被管设备拥有所有权限，除此之外还负责对证书服务器进行管理；数据库管理员可以对本地策略库进行编辑、修改，但不允许对被管设备进行操作；一般用户只允许查看某些设备的状态，不允许对被管设备进行操作。与此对应，我们定义了3个用户组：Root，DbManager，User，系统中所有的用户都属于这3个组之一。

3.3.1 *策略的定义和表示* 安全策略用来保护系统中的资源访问，说明不同组的用户允许做什么，不允许做什么，而凭证就是由凭证发放者签名过的策略，它用来将信任委托给凭证发放者所信任的第三方。一个策略片断如下所示：

```
〈? xml version="1.0"?〉
〈Policy〉
  〈Group name="Root"/〉
  〈Authorizer〉
    POLICY
  〈/Authorizer〉
  〈Licensees〉
    DSA:1f203ee5gh8tbabd117ffe
  〈/Licensees〉
  〈Comment〉
    Root is authorized to set the firewall 202.119.36.249
  〈/Comment〉
  〈Conditions〉
    〈application〉
      SecurityManager
    〈/application〉
    〈device〉FireWall〈/device〉
    〈ipAddress〉
      202.119.36.249
    〈/ipAddress〉
    〈operation〉set〈/operation〉
  〈/Conditions〉
〈/Policy〉
```

上面策略所表达的意思是：Root组用户由本地POLICY授权，可以对IP地址为202.119.36.249的防火墙进行配置工作。其中的几个标签是系统定义的，其含义分别为：

POLICY：本XML文件表示一个策略；Group：有关名字为name的组的一些信息；Authorizer：该组由谁授权，一般是本地POLICY或其他组的公钥；Licensees：实体，签名者的公钥；Comment：一些注释信息；Conditions：信任表述，一些行为属性。

3.3.2 *凭证的定义和表示* Root可以授权给DbManager和User使他们拥有未授权时所没有的权限，而授权则是通过凭证来实现的。凭证本质上就是由某个组签名的证书，主要用于将信任委托给可信者，比如：Root组用户相信DbManager组用户不会对防火墙进行有危险的操作，将其对IP地址为202.119.36.249的防火墙的配置权限委托给DbManager用户，该凭证可以表示如下：

```
〈?xml version="1.0"?〉
〈Credential〉
  〈Group name="DbManager"/〉
  〈Authorizer〉
    DSA:1f203ee5gh8tbabd117ffe
  〈/Authorizer〉
  〈Licensees〉
    DSA:gfb6yh8uabbd988rtii
  〈/Licensees〉
  〈Comment〉
    DbManager is authorized by Root to set the firewall
    202.119.36.249
  〈/Comment〉
  〈Conditions〉
    〈application〉
      SecurityManager
    〈/application〉
    〈device〉FireWall〈/device〉
    〈ipAddress〉
      202.119.36.249
    〈/ipAddress〉
    〈operation〉set〈/operation〉
  〈/Conditions〉
  〈Signature〉
    093a3134ffa38172200333110a2bc
  〈/Signature〉
〈/Credential〉
```

凭证与策略有着相同的语义结构，对照前面策略的XML表述，可以发现该凭证表示中的Authorizer元素的值是上述策略中Licensees的值即Root组的公钥，而相应地，凭证也多了一个Signature元素，表示发放该凭证者的数字签名。

3.3.3 *一致性检测算法* TME接收上述的凭证集和策略，对本地策略和凭证集进行解析，如果能够找到从请求者提交的凭证到本地策略的一条信任路径，则返回给XML/SNMP转换网关同意该请求的结果；否则，拒绝该请求。系统中的授权关系最终会形成一条信任链，信任链有两种类型：1) 直接信任链：所请求操作直接由本地POLICY进行授权，这种授权很简单，只需要直接解析策略文档即可；2) 传递信任

(下转第58页)

16 Du W, Deng J, Han Y S, et al. A Key Management Scheme for wireless Sensor Networks Using Deploying Knowledge. In: Proc. of INFOCOM2004. Hong Kong: IEEE Computer society, March 2004. 172～183
17 Liu D, Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In: Proc. of the 10th Annual Network and Distributed System Security Symposium (NDSS2003). San Diego, California: Internet Society Press, February 2003. 263～276
18 Bohge M, Trappe W. An Authentication framework for Hierarchical Ad Hoc Sensor Networks. In: Proc. of ACM Workshop on Wireless Security (WISE'03). San diego, California, USA: ACM Press, Sep. 2003. 79～87
19 Wood A, Stankovic J. Denial of Service in sensor networks. IEEE Computer, 2002, 35(10): 54～62
20 Douceur J R. The sybil attack. In: Proc. of First International workshop on Peer-to-peer systems (IPTPS'02). Cambridge MA, USA: Springer-Verlag, Volume 2429 of Lecture Notes in computer Science, 2002. 251～260
21 Newsome J, Shi E, Song D, et al. The Sybil Attack in Sensor Networks Analysis & Defenses. In: Proc. of Third Intl. Symposium on Information Processing in Sensor Natworks (IPSN'04). Berkeley, California, USA: ACM Press, April 2004. 259～268
22 Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and counter-measures. In: First IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA 2003). Anchorage, AK, USA: IEEE computer Society, May 2003. 113～127
23 Hu Y C, Perrig A, Johnson D B. Wormhole detection in wireless ad hoc networks: [Technical report TR01-384]. Department of Computer Science, Rice University, June 2002
24 Hu Y-C, Perrig A, Johnson D B. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In: Proc. of the Twenty-second Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003). San Francisco, CA: IEEE computer Society, 2003, 3: 1976～1986
25 Kwok J. A Wireless Protocol to Prevent Wormhole Attacks. A Thesis in TCC 402 Pressented to the Faculty of the School of Engineering and Applied Science University of Virginia, March 2004. 1～52. Available at: www. sc. virginia. edu/～evans/theses/dwok. pdf
26 Hu L, Evans D. Using Directional Antennas to Prevent Wormhole Attacks. In: Proc. of the 11th Annual Network and Distributed System Security Symposium (NDSS2004). San Diego, Cailfornia: Internet Society Press, Feb. 2004. 144～154
27 Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, energy-efficient multipath routing in woreless sensor networks. Mobile Computing and Communications Review, 2001, 4(5): 1～3

（上接第53页）

链：该信任链以本地策略 POLICY 为根，向下一级一级进行扩展，最后的叶子结点为当前所请求操作的公钥。两种信任链如图3所示。

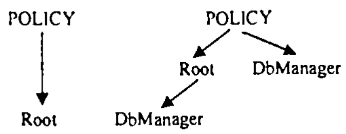

图3　直接信任链与传递信任链

TME 中一致性检测算法的目的就在于要在本地策略库和所搜集的凭证集中找出一条信任链，该信任链以本地策略 POLICY 为根。根据当前所请求操作的凭证或策略的 XML 文档，一致性检测算法提取出其中的 Authorizer 及 Licensees 元素，再根据这些元素的值搜索上一级授权者，一直到最后一级，如果最后一级授权者为关键字 POLICY，则一致性检测成功，向 XML/SNMP 转换网关返回结果允许该操作，否则拒绝该操作请求。具体算法描述如下：

a）一致性检测算法首先逐一分析所搜集到的凭证集（由 XML/SNMP 转换网关传入）；从每个凭证中解析出如下几个元素：Authorizer，Licensees，operation，Signature，并将这些元素存到一个数组 Trust 里面；

b）解析完所有凭证之后，分析 Trust 数组，从所请求操作的 Authorizer 所在数组元素开始，验证该元素里的 Signature 域，并逐级往上搜索 Licensees 域与本级 Authorizer 域相同的数组元素，一直到找到 Authorizer 域为 POLICY 为止，在上面搜索的过程中所搜索到的数组元素形成了一条信任链 t，如果在搜索过程中所有 Signature 域均合法，最后成功找到 Authorizer 域为 POLICY 的元素，并且信任链 t 上的所有元素的 operation 域均相同，则向 XML/SNMP 转换网关返回同意该请求的结果，然后将该信任链加上成功标记并写入本地信任库；

c）若上述步骤中任何一步验证不合法或出错，则向 XML/SNMP 转换网关返回出错，拒绝该请求，将该信任链加上失败标记写入本地信任库。

结束语　通过分析当前安全管理系统中存在的问题，本文讨论了安全管理系统中引入信任管理的必要性，并在本课题组所提出的基于 XML 的安全管理平台中引入了信任管理机制，提高了安全管理平台自身的安全性。针对基于 XML 的安全管理平台对自身安全的特殊要求，扩展了传统的基于策略的信任模型，加入了本地信任库和双向信任的机制，实现了安全管理平台中客户方与服务方的相互信任，并为下一步信任度评估的研究提供了基础。

信任机制在安全管理中的应用是一个崭新的研究课题，在基于 XML 的安全管理平台的研究中，我们在深入了解了信任管理以及相关领域的研究现状的基础上，做了一些尝试和改进，未来的工作主要集中在以下几个方面：基于历史声誉的信任度模型，改进一致性检测算法；性能测评和改进。

参考文献

1 Cisco Secure Policy Manager. http://www. cisco. com/warp/public/cc/pd/sqsw/sqppmn/index. shtml
2 Tivoli http://www-306. ibm. com/software/tivoli/
3 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. In: Proc. 17th Symposium on Security and Privacy. Oakland: IEEE, 1996. 164～173
4 Blaze M, Feigenbaum J, Strauss M. Compliance Checking in the PolicyMaker Trust Management System. Financial Cryptography 1998. 254～274
5 徐锋，吕建. Web 安全中的信任管理研究与进展. 软件学报，2002，13(11)：2057～2064
6 徐锋，吕建，等. 一个软件服务协同中的信任管理框架设计. 计算机科学，2003，30(9)：152～154
7 Blaze M, Ioannidis J, Keromytis A D. Experience with the KeyNote Trust Management System: Applications and Future Directions. iTrust 2003. 284～300
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 Intl. Workshop. Berlin: Springer-Verglag, 1999. 59～63
9 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A D. The KeyNote Trust Management System Version 2. Internet RFC 2704. http://www. faqs. org/rfcs/rfc2704. html, Sep. 1999
10 Chu Y-, Feigenbaum J, LaMacchia B, Resnick P, Strauss M. REFEREE: Trust Management for Web Applications. World Wide Web Journal, 1997, 2(2): 127～139
11 IBM. IBM Trust Establishment Policy Language. http://www. hrl. il. ibm. com/TrustEstablishment/PolicyLanguage. asp
12 Grandison T, Sloman M. A Survey of Trust in Internet Applications. IEEE Communications Surveys and Tutorials, 2000, 4(4): 2～16