计算机研究与发展 ISSN 1000-1239/CN 11-1777/TP
Journal of Computer Research and Development 45(12): 2033-2043, 2008

可信网络中用户行为可信的研究

林 闯[1] 田立勤[1,2] 王元卓[1]
[1](清华大学计算机科学与技术系 北京 100084)
[2](北京科技大学信息工程学院 北京 100083)
(chlin@tsinghua.edu.cn)

Research on User Behavior Trust in Trustworthy Network

Lin Chuang[1], Tian Liqin[1,2], and Wang Yuanzhuo[1]
[1](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)
[2](*School of Information Engineering, University of Science and Technology Beijing, Beijing* 100083)

Abstract With the increasing development of the computer network application, network security is facing the heavy challenge. The international research shows that network security is on the way to trustworthy network (TN). Apart from current security mechanism, the future TN adds behavior trust. TN includes the trust of service providers, the trust of the network information transmission and the trust of end-users. Trust based on user behavior not only can reduce or avoid the contact with the malicious user, but also can reduce the monitoring and prevention additional costs for mutual trust between the service providers and users, so research on user behavior trust will not only improve network security, but also improve overall network performance. In this paper, user behavior trust in trustworthy network is discussed. The authors systematically put forward a framework for evaluation, prediction and control of user behaviors, including reliable evaluation of user behavior trust, trust prediction to meet different prediction combinations of performance and security for service providers, trust and risk decision-making based on game theory, the mechanism based on the RBAC(role-based access control) model through the introduction of user behavior trust, simple and effective user behavior monitoring and prevention strategy based on user behavior trust, etc. Through effective combination of these user behavior trust management mechanisms, the unity of static and dynamic control and the unity of trust and risk, are implemented, which will lay the foundation for further study of the trustworthy network.

Key words trustworthy network; user behavior trust; evaluation of behavior trust; prediction of behavior trust; control of behavior

摘 要 目前网络安全受到严重的挑战,国际研究表明网络安全正向着网络可信方向发展,未来网络安全是增加行为可信的可信网络,它主要包括服务提供者的可信、网络信息传输的可信和终端用户的可信.通过研究用户的行为信任,不仅可以减少或避免与恶意用户交往,而且因为服务提供者与用户之间建立了互信,从而提高了它们合作完成任务的可能性,降低了因不信任带来的监控和防范等额外开销,所以对用户行为可信的研究不仅可以提高网络的安全性而且也可以提高网络的性能.以可信网络中用户行为可信研究为核心,提出了面向可信网络的用户行为信任的评估、预测与控制架构,包括行为信任的可靠评估;满足不同安全与性能需求的灵活的信任预测;基于信任与风险、利益得失的系统访问博弈决策;基于信任的动态的资源访问控制和以信任预防为主,实时监控为辅的异常行为的监控与防范等.

收稿日期:2008-11-22
基金项目:国家"九七三"重点基础研究发展规划基金项目(2006CB708301);国家自然科学基金项目(90718040, 60872055, 60673187, 60803123);教育部科技创新培育重点基金项目(707005);河北省科学技术研究与发展指导计划基金项目(07213570)

并把这些用户行为可信管理机制进行有效组合,实现了动态控制与静态控制,信任与风险的统一,为可信网络的进一步研究提供基础.

关键词 可信网络;用户行为信任;用户行为信任评估;用户行为信任预测;行为控制

中图法分类号 TP393

随着网络技术和应用的飞速发展,互联网日益呈现出复杂、异构等特点,当前的网络体系结构暴露出严重的不足,网络正面临着严峻的安全和服务质量(QoS)保障等重大挑战.随着网络技术的快速发展以及新应用的不断涌现,曾被大家普遍接受的网络自由主义理念和管理的无政府状态正在经历着严重挑战,并且不再适应当前实际的网络发展.重新思考网络体系结构已经成为国际研究界的共识,特别是围绕如何保障网络的可信性更是一个研究热点.国际研究表明[1-9]网络安全正向着网络可信方向发展,未来网络安全是增加行为可信的可信网络,这也是网络安全研究领域近年来取得的一个新的共识.

正如美国工程院院士 David Patterson 教授所指出:"过去的研究以追求高效行为为目标,而今天计算机系统需要建立高可信的网络服务,可信性必须成为可以衡量和验证的性能"[10-12].在网络领域里,正式提出以建立"高可信网络"为目标的计划则来自中国,旨在以高可信网络满足"高可信"质量水准的应用服务需要.目前"高可信网络"已被正式写进中国国务院公布的《国家中长期科学和技术发展规划纲要(2006—2020 年)》[13].《纲要》明确指出:"以发展高可信网络为重点,开发网络信息安全技术及相关产品,建立信息安全技术保障体系,防范各种信息安全突发事件".

为了提高美国的信息安全和信息信任,美国国家研究委员会提出信息空间信任研究建议[1],同时美国国家自然科学基金在 2007 年支持信息空间信任的研究项目[2].我国在上述领域也进行了多年的研究,国内也有一些公司已经开始在可信计算终端和网络安全方面开展工作,第 3 届中国可信计算与信息安全学术会议于 2008 年 10 月成功召开[3],但可信计算目前只提供了计算机平台的可信[4],不能提供整个网络可信,需要进一步将可信扩展到整个网络.2008 年,国家自然科学基金项目也重点强调了网络可信方面的内容[5],清华大学计算机系的网络控制研究组先后提出了可信网络[6],可信网络发展与科学问题研究[7],用户行为可信的评估、预测与控制[8-9],从可信计算到可信网络[14],可控可信可扩展的新一代互联网体系[15],网络安全的随机模型与评价技术[16-18]等相关方面进行了大量的前瞻性的研究.

目前业界对可信网络有不同理解:1)认为可信网络是基于认证的可信;2)认为是基于现有安全技术的整合;3)认为是网络的内容可信;4)认为是网络本身的可信;5)认为是网络上提供服务的可信等等.这种对可信网络的不同理解需要一个有效、现实、共同认可的可信网络概念达成共识,从而形成合力解决网络的信任问题.

可信网络最初是由作者在《计算机学报》"可信网络研究"一文中提出来的[6],可信网络的定义是:网络信息传输,服务提供者和用户的行为及其结果总是可以预期与可控制的,即能够做到行为状态可监测、行为结果可评估、异常行为可控制的.具体而言,网络的可信性应该包括一组属性,从用户的角度需要保障服务的安全性和可生存性,从设计的角度则需要提供网络的可管理性.相比传统的网络安全概念,可信性内涵更深:安全是一种外在表现的断言,可信则是经过行为过程分析得到的一种可度量的属性.

可信网络研究的内容主要包括 3 个方面:服务提供者的可信、网络信息传输的可信性和终端用户的可信.其中用户的可信又包括用户的身份和行为可信.用户身份可信是指终端用户的身份可以被准确鉴定,不被他人冒充,即终端用户的身份真实有效.终端用户的行为可信是指终端用户的行为是否可以评估、可预期、可管理、对网络设备和数据是否会造成破坏或毁坏.传统的安全机制可以解决用户的身份信任问题,但并不能处理用户的行为信任问题.例如在数字化电子资源的订购方面,大学生通过可信的身份信任(一般是学校的 IP 地址)可以登录到学校定购的数字资源服务器上,但他的行为却有可能是不可信的,例如,一些学生在校内常常使用网络下载工具大批量下载学校购买的电子资源或者私设代理服务器牟取非法所得等,即用户的身份是可信的,但用户的行为信任不一定可信.

研究用户行为可信首先是明确可信网络的需求,传统的授权与认证主要解决了用户的身份信任问题,但并没有解决用户的行为信任问题.可信网络必须在传统用户身份信任研究的基础上研究用户的行为信任,同时由于行为信任不仅比身份信任的控制粒度更细更具体,而且它是一种动态的信任形式,

因此在可信网络中需要研究用户的行为信任. 其次, 如果从可信网络的服务提供者、网络本身和网络用户 3 个组成信息系统层面上来看, 现有的保护措施是逐层递减的, 这说明人们往往把过多的注意力放在对服务提供者和网络的保护上, 而忽略了用户的安全问题, 这显然是不合理的. 因为用户不仅是创建和存放重要数据的源头, 同时绝大多数的攻击事件也都是从用户端发起的. 第三, 近年来的网络应用经验表明网络安全不是信息安全的全部, 内容安全也占相当重要的部分. 如果用户间的信息内容不能得到保证, 即使网络是很安全的, 信息安全也无法保障. 第四, 研究用户行为信任可以在用户没有进行任何破坏行为之前提前预测用户的行为, 即检测控制具有主动性和行为的预见性, 而不是像入侵检测那样要等检测到不法行为发生时才开始阻止破坏行为的发生. 第五, 对用户行为信任的研究, 不仅可以通过减少或避免与恶意用户的交往来提高网络的安全性, 而且因为服务提供者与用户之间建立了互信, 从而提高了他们间合作完成任务的可能性, 简化了因不信任带来的监控和防范等额外开销, 因此用户行为信任的研究不仅可以提高网络的安全性而且也可以提高网络的整体性能.

1　整体架构与基本准则

1.1　用户行为可信的整体结构

研究用户行为可信问题主要包括用户行为信任的评估、预测和控制, 其中用户行为信任评估是基础, 用户行为可信控制是目的, 其整体结构见图 1:

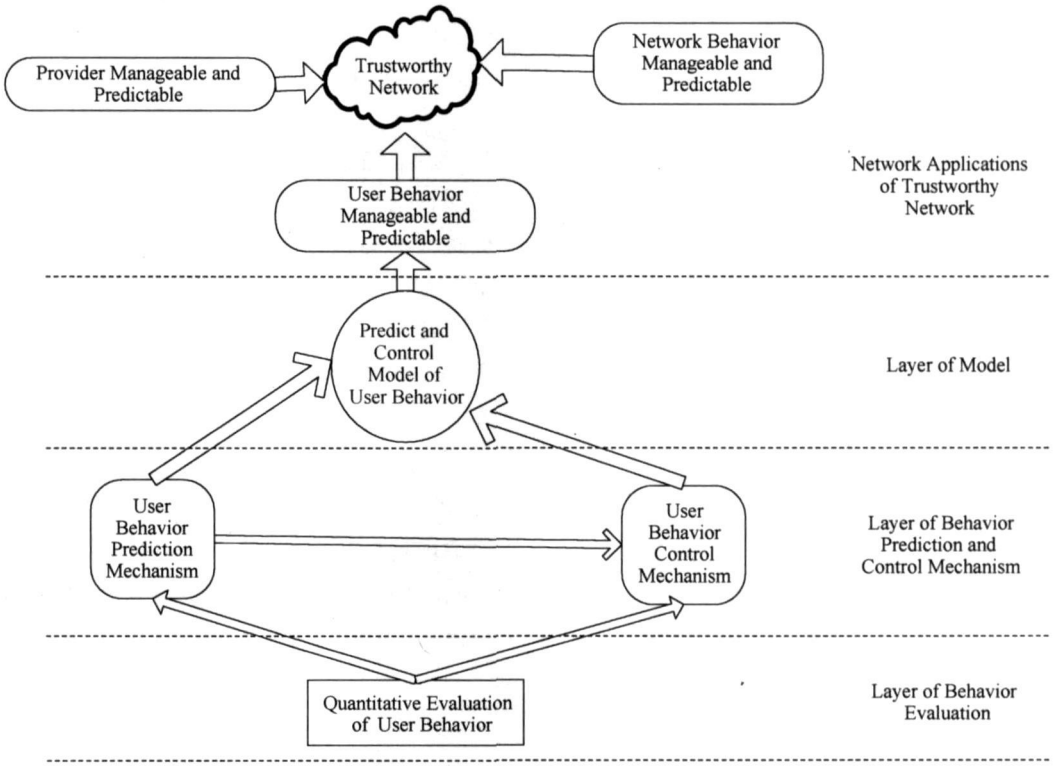

Fig. 1　The overall structure of the research on user behavior trust.

图 1　用户行为可信研究的整体结构

1.2　用户行为可信的基本准则

根据可信网络的基本要求, 我们可以得出用户行为可信的基本准则, 有了准则我们就能围绕这些准则进行进一步细致的研究, 这些准则主要包括:

1) 信任评估的客观性. 信任是从社会科学中借鉴过来的, 主观性过多会影响信任评估的可信度, 因此评估应该是主客观相结合的, 即信任评估的评价是主观的, 但内容必须是客观的, 兼顾信任的主客观特性.

2) 主观的一致性. 当用户行为信任评估中主观性参数较多时, 需要提供主观性的一致性检查, 保证评估结果的科学性和合理性.

3) 信任评估的规模性. 用户行为的信任评估应该是基于用户长期大量的行为, 因为只有通过大量的用户行为得来的评估结果才具有稳定性和代表性的"性格特性", 才能作为我们控制的依据, 强调"日久见人心"的社会信任特性.

4) 评估考虑行为的价值性. 考虑用户行为的价值

是防止恶意用户用低价值的访问换取高信任, 然后用高信任进行高价值行为欺骗.

5) 信任评估的时间特性. 信任评估要考虑近期用户行为的重要性和远期行为的衰减性等时间特性.

6) 信任评估的防欺骗. 防范恶意用户以少数次、低价值访问来换取高信任等的欺骗, 通常采取保守的"慢升"信任值的方法来防范欺骗.

7) 信任评估的欺骗惩罚. 不仅要防范欺骗, 同时对已经发生欺骗的行为要进行惩罚, 通常采取大幅度的"快降"信任值的方法来惩罚欺骗.

8) 方法的可扩展性. 这与要求用户行为的规模性是一对矛盾, 可信网络中用户行为证据是一个庞大的数据, 因此要解决可扩展性问题.

9) 信任信息的可共享性. 信任信息共享不仅可以加快对陌生用户的信任评估速度, 而且可以提高信任评估的可信度, 因此需要在各个不同服务提供者之间进行信任信息的共享与交换. 主要解决信任的主观性带来的信任信息难以共享的问题.

10) 行为证据的规范性. 各种行为证据的大小、方向性、单调性、含义各不相同, 要对其进行统一规范化处理.

11) 控制效果与性能折中性. 用户行为控制应具有主动性和预见性, 而不是要等检测到了不法行为发生时才开始阻止破坏行为的发生, 基本思路是以预防为主, 以监控为辅, 这样可以兼顾控制的效果与性能两大问题.

12) 防风险性. 信任与风险是一对矛盾的统一体, 在信任的基础上需要进行风险分析.

2 用户行为可信管理的机制

保证用户行为可信的基本思路是多层次的可信控制的有效组合, 各种可信控制内容和方法相互补充, 相互配合, 最终达到管理用户行为可信的目的, 它包括历史行为的可信评估, 未来行为可信的预测, 实时行为可信的监控, 信任与风险的评估以及基于信任的资源访问控制等多种可信管理的合理组合, 下面分别论述.

2.1 基于用户行为信任的可信管理

基于用户以往行为信任的可信管理主要是设计出符合可信准则的行为信任评估策略, 我们这里论述一种基于滑动窗口的用户行为信任的评估策略, 保证用户行为的信任评估是基于用户大量行为表现的. 我们利用滑动窗口大小来体现用户行为信任评估的时间和空间特性, 它既可以保证用户行为信任评估的规模性也可以保证行为信任评估的可扩展性, 根据窗口记录的时间来保证近期行为的重要性和远期行为的衰减性, 同时根据窗口的移动与更新来防止用户的欺骗以及对欺骗的惩罚等, 窗口的基本模型如图 2 所示:

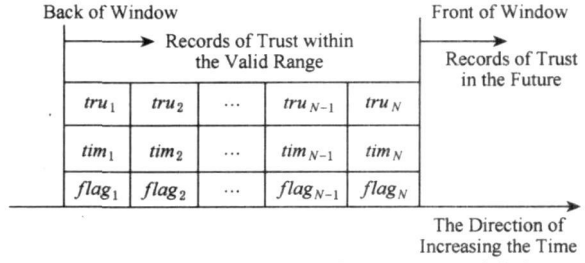

Fig. 2 The sliding window of evaluation of behavior trust.

图 2 行为信任评估的滑动窗口

1) 窗口的大小

窗口的大小是 N, 当用户访问的次数 m 很大时, 只保留窗口大小的 N 条访问信任记录, 这样可以保证信任评估的可扩展性. 当欺骗者企图通过次数较少的高信任交往以获得最终高信任评估值时, 由于总的评估值是按全部 N 次计算的, 所以即使每次交往获得很高的信任评估值, 由于实际交往的次数 m 远比 N 小, 所以并不能很快获得高信任值, 体现了日久见人心的信任特性.

2) 窗口的初始化

窗口的每个用户的信任值被初始化为陌生用户的不确定信任 $uncer\_tru$, 这种用户享有较低的系统访问权限, 随着用户访问的到来, 初始化值逐渐移出窗口, 实际用户信任记录逐渐移入窗口.

3) 基于信任过期的窗口更新

当用户长时间不访问时, 一些信任记录离当前时间越来越远, 逐渐成为过期信任记录, 信任是否过期是通过比较最新信任记录时间与各个记录时间的差是否大于有效时间段 $Valid\_Tim$ 来决定的, 过期信任记录的值被替换为陌生信任记录的值, 这样随时间的推移信任会逐渐趋于陌生信任值, 这也是信任评估的一个基本特性——陌生信任值的趋向性. 替换策略采用最远时间替换策略, 即, 窗口中空出来的记录的值替换为陌生用户信任值, 时间与最左边的有效记录时间 tim_1 相同. 这样不仅能最大限度保证有效的信任记录不被提前挤出窗口, 而且可以提高信任评估的有效率.

4) 基于新信任触发的窗口更新

基于新信任的内容更新的基本思路是: 当有新的用户访问信任记录到来时, 通过窗口的右移, 把时间最长的最左边记录移出, 新的记录值移入窗口的最右边, 保证评估的可扩展性, 同时, 对最左边移出的信任记录进行累加, 累加的结果也参与最终的信任计算, 也就是说, 过期的信任并不是完全被"抛弃", 只是在计算中所占比例减小了.

5) 基于滑动窗口的行为信任计算

首先计算窗口内用户行为的 m 个信任记录的综合信任值 m_tru, 用户行为包括标志为 $norm$ 用户实际行为信任值和标志记为 $punish$ 信任惩罚记录, 计算的基本思路是越近期的信任其在综合的信任评估中所占比重越大, 每次的信任值在总的信任中所占的比例与该信任记录的时间成正比, 用式(1)计算:

$$m\_tru = \sum_{j=1}^{m} \frac{(tim_j - tim_1)}{\sum_{j=1}^{m}(tim_j - tim_1)} tru_j. \quad (1)$$

其次, 计算窗口内所有 N(N 是窗口的大小)个信任记录的信任值, 用式(2)计算:

$$N\_tru = \sum_{i=1}^{N} \frac{(tim_i - tim_0)}{\sum_{i}^{N}(tim_i - tim_0)} tru_i. \quad (2)$$

有了 m_tru 和 N_tru 后就可以计算窗口内的综合信任值, 基本策略是保守的最小化策略, 即取上面两者的最小值, 这样既可以防止恶意用户用少数次交往形成的高信任值的欺骗行为, 也可以体现不信任用户的真实信任值. 最后还要考虑对不信任记录惩罚: 如果某次行为被评估为不信任, 则根据信任控制的粒度和具体控制的要求将若干次已经是信任的评估值降为不信任 min_tru, 使整体信任值快速下降, 达到对不信任行为进行惩罚的目的.

2.2　基于不同需求预测的可信管理

由于用户行为信任的评估是基于过去交往的行为证据之上, 而我们需要的是未来的用户行为信任等级, 因此科学地预测未来用户的行为信任等级是非常必要的. 同时服务提供者可以根据对用户性能和安全等信任的不同需求进行更细、更具体、更灵活的预测要求. 这样要求能实现可配置的满足不同需求的用户行为信任的预测策略, 由于贝叶斯网络模型一方面它可以将用户行为信任预测的因果知识直接用有向图自然直观地表示出来, 另一方面, 也可以将以往用户行为的统计数据以条件概率的形式融入模型, 这样贝叶斯网络就能将用户行为的先验知识和后验的数据无缝地结合在一起, 并能够达到满足不同需求组合的细粒度的预测效果.

1) 用户行为信任的贝叶斯网络模型

一个用户行为信任预测的贝叶斯基本网络模型是一个有向无环图(见图 3), 它由代表变量节点及连接这些节点有向边构成. 变量节点包括要预测的用户行为的总体信任 T 及其分解后的信任属性, 如用户效率(性能)属性 P 及用户安全属性 S 等. 节点间的有向边代表了节点间的相互关系, 由父节点指向其后代节点, 父节点是用户行为总体信任 T, 叶节点是用户行为信任的各种信任属性.

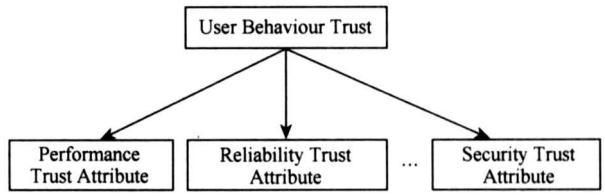

Fig. 3　The Bayesian network model of prediction.

图 3　预测的贝叶斯网络模型

2) 用户行为信任预测的数据结构

为了能有效地对用户行为信任进行预测, 将用户行为信任 T、性能属性 P 和安全属性 S 等各个节点划分为 L 个信任等级. 每次交往后, 交往的总次数 n 加 1, 节点行为信任评估的值落在哪个范围内, 则相应范围内所对应的次数加 1, 其他保持不变. 为了满足各种不同要求的预测, 我们还要保存两个和两个以上的不同节点值同时落在的不同范围的次数, 这主要用来计算在多个信任属性条件下的用户行为信任的预测问题. 节点值同时落在两个不同节点范围内的次数用二维数组存储, 节点值同时落在 3 个或 4 个不同节点范围内的次数分别用三维或四维数组存储. 数组的名字表示不同的节点, 数组的下标表示不同的信任等级范围, 我们用 $|T_i|$, $|P_i|$ 和 $|S_i|$ ($1 \leqslant i \leqslant L$)分别表示与所预测用户的交往历史中整体信任、性能属性和安全属性的值分别落在 T_i, P_i 和 S_i 范围内的次数, 用 $p(T_i)$, $p(P_i)$, $p(S_i)$ 分别表示它们的概率.

3) 用户行为信任预测的先验数据的计算

① 用户行为信任的先验概率

用户行为信任的先验概率的计算见式(3):

$$p\left(T_i\right) \frac{|T_i|}{n}, \quad 1 \leqslant i \leqslant L,$$

并且

$$\sum_{i=1}^{L} p\left(T_i\right) = 1. \quad (3)$$

② 用户行为属性的先验概率

用户行为属性的先验概率的计算见式(4),这里以安全属性为例,其他信任属性的计算方法相似:

$$p\left(S_i\right)\ \frac{|S_i|}{n},\ 1\leqslant i\leqslant L,$$

并且

$$\sum_{i=1}^{L} p\left(S_i\right)\ =1. \tag{4}$$

③ 节点的条件概率表

除了计算先验概率外,还必须计算各节点的条件概率,对于叶节点来说,每个叶节点都有一个条件概率表.以计算 $p(S_i/T_j)$ 条件概率为例,它表示用户根节点在 T_j 这个信任范围内的条件下安全信任属性节点在 S_i 信任范围内的概率.由式(5)计算获得:

$$p(S_i/T_j)=\frac{p(S_i,\ T_j)}{p(T_j)}=\frac{|S_i\cap T_j|/n}{|T_j|/n}=\frac{|S_i\cap T_j|}{|T_j|}. \tag{5}$$

4) 满足不同安全和性能任意条件组合的用户信任的预测

利用贝叶斯公式,我们也可以预测不同安全和性能组合的用户信任等级概率,例如,我们仍然假设 $L=5$,即非常信任(信任等级为 1)、信任(信任等级为 2)、比较信任(信任等级为 3)、基本信任(信任等级为 4)和不信任(信任等级为 5),那么我们用 $p(T_1/P_3,\ S_2)$ 可以求出关于性能信任属性为"比较信任"(信任等级是 3),安全信任属性为"信任"(信任等级是 2)的条件下,用户总体行为信任为"非常信任"(信任等级是 1)的概率.双信任属性条件下的用户行为信任的计算见式(6):

$$p\left(T_i/P_j,\ S_k\right)=\frac{p\left(P_j,\ S_k/T_i\right)p\left(T_i\right)}{p\left(P_j,\ S_k\right)}=\frac{p\left(P_j,\ S_k,\ T_i\right)}{p\left(P_j,\ S_k\right)}=\frac{|P_j\cap S_k\cap T_i|}{n}\Big/\frac{|P_j\cap S_k|}{n}=\frac{|P_j\cap S_k\cap T_i|}{|P_j\cap S_k|}. \tag{6}$$

2.3 基于风险与收益的可信管理

由于信任和风险是并存的,单独依靠预测的信任等级进行决策是非常片面和危险的,因此在控制决策中还必须对风险进行分析,将用户的行为信任的预测结果、可能的收益情况进行博弈分析找出纳什均衡策略,计算出控制用户行为的决策条件.

1) 双方利益的得失分析

由于用户安全行为信任属性是用户行为信任中最重要的内容,因此主要论述用户安全行为信任属性的博弈分析问题,其中的实例和解释说明是以学校提供的数字资源为例的.先介绍文中用到的符号所代表的意义.

$Sloss_{acc}^{dec}>0$——表示服务提供者在接受用户的欺骗访问时可能受到的平均损失量.如过量下载数字资源,私设对外代理服务器等,其他的欺骗也包括网络安全攻击导致服务器无法提供正常的服务或资源访问等.

$Sincome_{acc}^{n\_dec}$——表示服务提供者接受用户的不欺骗访问时,服务提供者可能得到正常的平均收益.如有偿数字资源服务下载、广告、帮助用户检索等获得的收益等.

$Sloss_{n\_acc}^{n\_dec}>0$——表示服务提供者拒绝接受且用户不欺骗访问时服务提供者可能受到的平均损失.如数字资源服务因为拒绝正常的用户访问而使数字资源没有得到充分利用,以及双方由此引起的互不信任所造成的不合作损失等.

$Uincome_{acc}^{dec}$——表示用户采取欺骗行为且服务提供者接受访问时用户得到的超额收益.如过量下载,私设对外代理服务器将数字资源转卖给第三方,获取其他用户的帐号信息,商业竞争者进行 DOS 攻击以提高自己的商业竞争力等获得的额外收益.

$Uincome_{acc}^{n\_dec}$——表示用户不欺骗且服务提供者接受访问时用户获得的平均收益.如下载相关的电子资源、浏览新闻和阅读专业资料等.

$Ucost>0$——用户采取欺骗行为所需要的成本.如购买相应的软件、学习欺骗的方法和技巧所需要的时间和精力等.

$Upunish>0$——表示用户采取欺骗行为所可能受到的惩罚.如停止用户对数据库的使用权或受到法律起诉等.通过分析我们可以得出如表 1 所示的服务提供者与用户之间的支付矩阵表,其中 i 为用户行为信任等级,其中 $\alpha_K\in[0,\ 1]$ 是博弈分析的参数因子,主要取决信任划分的等级粒度和对安全要求的强度,可以根据决策者的要求进行调整.

Table 1 Payment Matrix Between Provider and User

表 1 服务提供者与用户之间的支付矩阵表

User Provider	Cheat	No-Cheat
Receive	$(-Sloss_{acc}^{dec}\alpha_1^{i-1},\ Uincome_{acc}^{dec}\alpha_3^{i-1}+Uincome_{acc}^{n\_dec}\alpha_4^{i-1}-Ucost-Upunish\ \alpha_5^{i-1}$	$(Sincome_{acc}^{n\_dec}\alpha_2^{i-1},\ Uincome_{acc}^{n\_dec}\alpha_4^{i-1})$
No-Receive	$(0,\ -Ucost)$	$(-Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1},\ 0)$

下面考虑信任风险与收益的用户行为的可信控制条件.

已知用户行为的信任等级的预测概率 Pt 和服务提供者的支付矩阵,则服务提供者接受访问的控

制条件是:

$$\sum_{i=1}^{L} Pt_i[-y^* Sloss_{acc}^{dec}\alpha_1^{i-1} + (1-y^*)(Sincome_{acc}^{n\_dec}\alpha_2^{i-1})] > 0,$$

其中 Pt_i 是信任等级为 i 的预测概率, y^* 和 $1-y^*$ 分别是用户欺骗和不欺骗的混合纳什均衡策略, L 是信任等级划分的级别.

因为不同信任等级的用户其支付矩阵是不一样的, 因此决策前先必须预测用户在各信任等级的概率 Pt_i, 这个可以通过第 2.2 节的多信任属性不同条件下的预测公式计算出来, 这里不再赘述.

有了预测的用户信任等级概率, 我们还要用博弈理论分析用户的决策概率, 我们假定用户是理性的, 即用户寻求以一种最大化自己支付的方式进行博弈, 那么能达到这个要求并且双方可以持久保持稳定状态的就是混合策略的纳什均衡, 因此先计算用户的混合纳什均衡策略. 因为服务提供者的预期支付函数为:

$$E_S(\boldsymbol{P}_1, \boldsymbol{P}_2) = \boldsymbol{P}_1 \boldsymbol{A}_i \boldsymbol{P}_2^{\mathrm{T}} = (x, 1-x) \begin{pmatrix} -Sloss_{acc}^{dec}\alpha_1^{i-1} & Sincome_{acc}^{n\_dec}\alpha_2^{i-1} \\ 0 & -Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1} \end{pmatrix} \begin{pmatrix} y \\ 1-y \end{pmatrix} = -xySloss_{acc}^{dec}\alpha_1^{i-1} + x(1-y)Sincome_{acc}^{n\_dec}\alpha_2^{i-1} - (1-x)(1-y)Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1}.$$

对上式关于 x 求偏导, 可得用户最优化的一阶条件为

$$\frac{\partial E_S(\boldsymbol{P}_1, \boldsymbol{P}_2)}{\partial x} = Sincome_{acc}^{n\_dec}\alpha_2^{i-1} + Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1} - y(Sloss_{acc}^{dec}\alpha_1^{i-1} + Sincome_{acc}^{n\_dec}\alpha_2^{i-1} + Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1} = 0.$$

解得

$$y^* = \frac{(Sincome_{acc}^{n\_dec}\alpha_2^{i-1} + Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1})}{(Sloss_{acc}^{dec}\alpha_1^{i-1} + Sincome_{acc}^{n\_dec}\alpha_2^{i-1} + Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1})}.$$

即 $(y^*, 1-y^*)$ 是用户的混合纳什均衡策略.

由表 1 知, 用户信任等级为 i 的服务提供者的支付矩阵为:

$$\begin{pmatrix} -Sloss_{acc}^{dec}\alpha_1^{i-1} & Sincome_{acc}^{n\_dec}\alpha_2^{i-1} \\ 0 & -Sloss_{n\_acc}^{n\_dec}\alpha_6^{i-1} \end{pmatrix}.$$

现在求接收用户访问的决策条件, 实际就是求服务提供者的接受概率为 1, 用户选择欺骗和不欺骗的概率分别为 y^*, $1-y^*$ 时的服务提供者的利益得失情况, 此矩阵的第 1 行表示接受用户访问, 第 1 列表示用户欺骗, 第 2 列表示不欺骗, 因此服务提供者获得的利益为

$$-y^* Sloss_{acc}^{dec}\alpha_1^{i-1} + (1-y^*)Sincome_{acc}^{n\_dec}\alpha_2^{i-1}.$$

上式只是用户信任等级为 i 时服务提供者获得的利益结果, 要想得到该用户的全部获利情况, 就必须对 L 个信任等级进行加权求和, 即服务提供者总的获得的利益为

$$\sum_{i=1}^{L} Pt_i[-y^* Sloss_{acc}^{dec}\alpha_1^{i-1} + (1-y^*)(Sincome_{acc}^{n\_dec}\alpha_2^{i-1})]. \quad (7)$$

如果这个值大于零, 则说明服务提供者的收益大于零, 那么就接受访问, 否则拒绝访问.

2.4　基于行为信任的动态资源访问控制

1) 基本模型描述

基于用户行为信任的动态角色访问控制机制是在基于角色的访问控制中引入行为信任等属性, 克服了该模型的静态局限性, 实现了动态授权, 并缓解了角色扩散问题, 以适应未来可信网络用户动态性和数量大的特点, 其结构模型图如图 4 所示. 用户信任级别集的加入, 使该模型的授权不再是纯粹基于身份信任的静态机制, 而成为基于身份信任和行为信任相结合的具有动态性的授权机制.

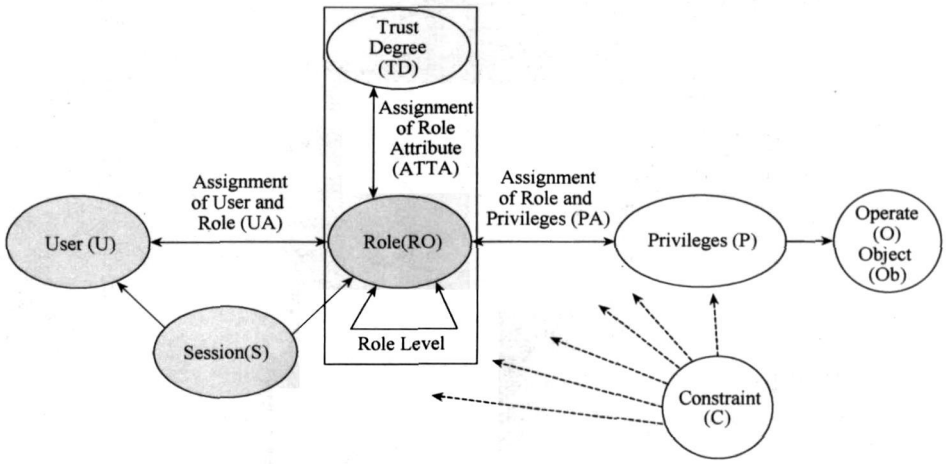

Fig. 4　Dynamic access control model based role.

图 4　基于行为信任的动态角色访问控制模型

2) 模型的授权

用户登录后,根据身份获得相应的角色,但此时角色还没有被指派信任属性值,角色也不拥有任何权限,用户不能进行任何操作.当得到用户的信任级别后,把它和其他的属性值作为角色属性赋予角色,然后通过权限查询获得相应的权限,此时,用户的角色才被激活,用户才能获得实际的操作权限.图 5 说明了模型的授权流程图:

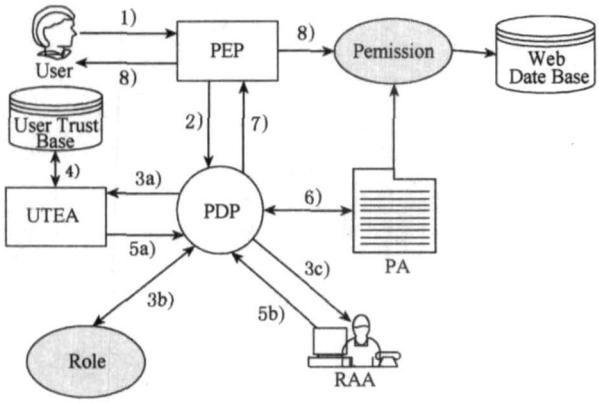

Fig. 5 Flow chart of authorization.

图 5 模型的授权流程图

主要分为以下几个步骤:

1) User(用户)向策略执行点(policy enforcement point, PEP)提交访问请求;2) PEP 向策略决策点(policy decision point, PDP)发出访问决策请求;3a) PDP 向用户信任评估代理(user trust evaluation agent, UTEA)发出用户信任评估请求;3b) PDP 根据身份获得该用户的角色;3c) PDP 向角色属性机构(role attribute authority, RAA)发出查询角色属性请求;4) UTEA 从用户信任库中取出该用户的信任等级;5a) UTEA 把用户信任级别发送给 PDP;5b) RAA 获取要求的各属性值,把结果发送给 PDP;6) PDP 把收到的用户信任级别和 RAA 发送的其他各属性值一并指派给该用户的角色,通过查询 PA(permission assignment)表,获得角色当前的权限;7) PDP 对比该权限与用户的请求权限是否相同或者是否包含用户的请求权限.如果相同或者该权限包含请求的权限,则允许此次访问请求;如果小于用户的请求权限,则拒绝这次访问请求,把决策结果发送给 PEP;8) PEP 执行 PDP 的决定,如果允许访问,激活该用户的角色;如果拒绝访问,则向用户返回拒绝信息.

2.5 结合行为信任和行为监控的可信管理

前面用户行为可信管理的目的是预防,但也要防止在实际访问过程中的意外反常行为情况的出现,不仅要防止恶意用户"放长线吊大鱼"的重大危害服务提供者系统的恶意事件的发生,而且要防止用户无意中的重大危害系统安全情况出现,因此我们必须将预防与实时监控结合起来,在用户行为信任评估的基础上,对用户访问过程中的实时异常行为进行监控与防范.实时监控的开销问题是研究实时监控必须解决的一个重要问题,由于我们事先已经有了用户行为信任的结果,因此可以根据用户行为信任的情况对实时监控进行必要的调控和简化,从而可以大大提高实时监控的性能.因此在用户行为信任以防范为主的基础上增加有效的异常行为的监控与防范策略是必要的,只有这种将预防与监控的合理结合才可以较好地解决用户的行为控制问题.

我们提出一种基于用户行为信任的简单有效的异常行为监控策略,区别于以往以大量用户行为的统计分布为基准的常规控制方法.我们将用户自己长期统计行为和所有用户的长期统计行为结合起来作为评判基准,来判断用户行为的异常,并根据用户行为信任的高低决定对用户行为采取实时监控的力度,提高了异常行为检测的准确度和速度.具体判断过程如下.

设实时获得的用户行为证据值为 tru_{new},最低信任值为 $thr0$,用户过去的该证据的累加证据值为 T_{ave},该证据的常规信任范围为(T_{tra1}, T_{tra2}),异常行为的偏离度为 D,则通过以下步骤判断该用户行为证据是否为异常:

1) 判断该证据 tru_{new} 的过去累加值 T_{ave} 是否可信,如果不可信,则判定该实时证据 tru_{new} 为不可信,参与本次实时监控最终结果的证据为更新后的累加证据 T_{ave}^{new}.如果可信则进入步骤 2),这个判断准则是将用户的实时行为与用户以往的信任结合起来.

2) 与该用户自己历史行为证据比较判断是否行为异常,看

$$|tru_{new} - T_{ave}| < D \tag{8}$$

是否成立,如果成立为可信证据,如果不成立则为预警的怀疑证据,转步骤 3)进一步判断.

3)与整个系统行为证据信任化的信任范围比较判断是否行为异常,看式(9)是否成立,如果成立则为可信证据,否则为不可信证据.

$$T_{tra1} < tru_{new} < T_{tra2}. \tag{9}$$

4) 各个异常行为的证据值按事先确定的权重进行组合,如果结果大于预定的阈值 T_{abnorm},则认为

该用户的实时行为是异常的, 对于异常的实时用户行为, 立即中断用户的访问权限.

3　用户行为可信管理的评估特性

1) 评估是方法的主观性和内容的客观性的统一

信任的主观性在算法评估中的各个可配置参数中得到充分体现, 如信任有效时间段 $Valid\_Tim$ 的长短、窗口 N 大小等. 由于信任评估的最根本依据是可测可量化的行为证据 $et\in[0,1]$, 这些证据具有客观性, 也是不同服务提供者之间共享信任信息的要素. 因此信任评估体现了主客观的有效结合.

2) 评估是交往次数的规模性和可扩展性的统一

评估的过程中根据实际评估的要求和评估的粒度事先确定最小交往次数, 在本文的算法中就是窗口的大小 N, 本文中通过下列措施达到防止恶意用户通过较少次数的高信任交往来骗取最终高信任评估值目的, 即, 当 $m<N$, 且 $N\_tru\leqslant m\_tru$ 时, 结果取 N_tru 而不是 m_tru. 对于可扩展性, 我们采用的方法是: 如果用户实际交往的次数 m 大于最大需要保留的行为记录次数 N 时, 就需要对大于 N 的历史行为信任记录进行截断, 保证信任评估的可扩展性. 由于我们截断的措施是按时间最远的顺序进行的, 因此对信任的评估影响达到最小, 同时被截去的信任记录也并没有完全丢弃, 而是累加到累加记录中, 参加最后的信任计算中. 这样达到用户行为信任评估的规模性和可扩展性的辨证结合.

3) 评估是近期行为的重要性和远期行为的衰减性的统一

本文在信任计算时, 一方面, 证据的权重是根据时间的近远逐渐递减, 另一方面当获得新的信任值时, 被移出窗口的信任是对应时间最远的, 这都体现了近期的行为表现对信任的评估具有较大的作用的特性.

当用户长时间不访问时, 窗口内因过期被移出去的信任记录逐渐被替换为陌生信任记录, 这样当用户长期不访问时, 信任会随时间的推移逐渐趋于陌生信任值, 实现信任随时间衰减的基本特性.

4) 评估值是"慢升"与"快降"的统一

本文是通过设置最小访问次数, 即窗口大小 N 来体现信任的"慢升", 从而防止恶意用户的欺骗, 如果用户只有少数几次的访问行为, 即使信任评估值 m_tru 很高, 它远远大于 N_tru, 但由于最后的信任值是按全部 N 个信任记录计算的, 所以不会上升

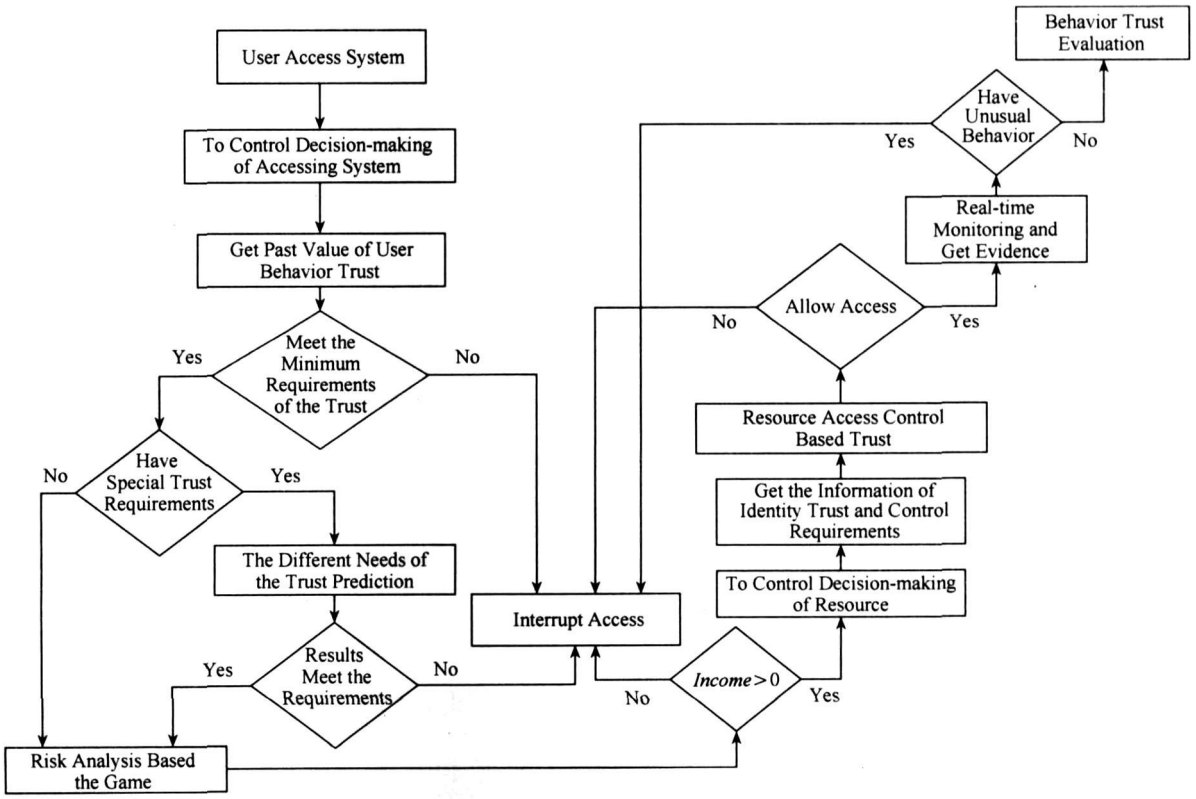

Fig. 6　Framework for control of user behavior in TN.

图 6　可信网络中用户行为信任控制架构

很快.对评为不信任的用户惩罚性地快速降低其信任值,本文选取时间最近的(窗口最右边的)k 个记录被降为不信任值 min_tru,由于降低信任值的力度远远大于逐渐增加信任的力度,因此体现了"慢升快降"的特性.

5) 多种行为可信管理机制的有效组合

用户行为可信控制的第 1 步是用户的身份信任,并将身份信任与本文的行为信任结合起来,对用户行为可信的管理是以上多种可信控制策略的多层次的有效组合,各种可信控制内容和方法相互补充,相互配合,最终达到管理用户行为可信的目的.可信网络中用户行为可信控制基本架构如图 6 所示,共有五大行为控制点,分别是:考虑用户总体行为信任,基于服务提供者对用户不同需求的信任预测,对信任进行风险的博弈分析,基于行为信任的资源访问控制和结合历史行为信任的异常行为的实时监控,其中前 3 种是系统访问的控制,第 4 种是资源的访问控制,最后一种是实时的监控,做到静态动态结合,历史与实时结合,信任与风险结合,过去与未来,控制效果与性能的有机结合.

4 进一步研究方向

随着可信网络研究的不断深入,用户行为可信的研究已越来越为人们所重视,如何提供面向可信网络的用户行为信任的评估、预测与控制架构,并通过多种用户行为可信管理机制的有效组合,达到控制的静态与动态、历史与实时、信任与风险的有效统一,已成为重要的研究方向,本文在用户行为可信的整体架构、可信管理机制以及评估特征等方面做了一些探索性的工作,但仍具有如下问题丞待解决:

1) 用户行为信任的形式化分析与验证

用户访问系统的时间、过程具有多样性、随机性等特点,同时,对用户行为信任的评估也有并发、顺序、循环和选择过程的描述对形式化描述方法提出了新的要求,建立适合用户行为信任的评估、预测和控制的形式化模型及验证方法是重要研究方向.

2) 区分不同服务提供者的用户行为信任评估

互联网的服务提供者具有大多数节点只有少量的连接,而极少数节点却有大量的连接的特点,对于重要服务者拥有大量的用户访问和充足的用户行为信任证据,如何解决评估中的可扩展性问题,而对于普通的服务提供者拥有用户少,证据也不充足,如何解决信任证据的共享问题,都是有待进一步研究的方向.

3) 移动用户行为的描述与评估

无需固定基础设施支持的自组织网络中节点可以随意移动,并且节点的能量和计算能力等资源有限.研究这种网络中用户行为信任关系框架面临巨大的挑战.

参 考 文 献

[1] Trust in Cyberspace [EB/OL]. [2006-07-08] http://www.nap.edu/catalog/6161.html

[2] CyberTrust [EB/OL]. [2007-03-05] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13451&org=CISE&from=home

[3] The Third China Trusted Computing and Information Securty 2008 [EB/OL]. [2008-10-09] http://www.tc2008.org/zwtz.htm (in Chinese)
(第三届中国可信计算与信息安全学术会议 CTCIS 2008 [EB/OL]. [2008-10-09] http://www.tc2008.org/zwtz.htm, 2008)

[4] Trusted Computing Group [EB/OL]. [2007-05-08] http://www.trustedcomputinggroup.org/home

[5] National Natural Science Foundation of China [EB/OL]. [2008-04-08] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2008xmzn/02zd/06xx.htm (in Chinese)
(2008 年度国家自然科学基金项目指南:重要项目[EB/OL]. [2008-04-08] http://www.nsfc.gov.cn/nsfc/cen/xmzn/2008xmzn/02zd/06xx.htm)

[6] Lin Chuang, Peng Xuehai. Research on trustworthy networks [J]. Chinese Journal of Computers, 2005, 28(5): 751-758 (in Chinese)
(林闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751-758)

[7] Lin Chuang, Wang Yuanzhuo, Tian Liqin. Development of trusted network and challenges it faces [J]. ZTE Communications, 2008, 6(1): 13-17

[8] Tian Liqin, Lin Chuang. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network [J]. Chinese Journal of Computers, 2007, 30(11): 1930-1938 (in Chinese)
(田立勤, 林闯. 可信网络中一种基于用户行为信任预测的博弈控制分析[J]. 计算机学报, 2007, 30(11): 1930-1938)

[9] Tian Liqin, Lin Chuang, Sun Jinxia. A kind of prediction method of user behavior for future trustworthy network [C]//Proc of the 10th Int Conf on Communication Technology (ICCT2006). Piscataway, NJ: IEEE, 2006: 199-202

[10] Recovery Oriented Computing [EB/OL]. [2006-12-18] http://www.stanford.edu, or http://roc.cs.berkeley.edu

[11] Global Environment for Networking Investigations [EB/OL]. [2007-08-08] http://geni.net/

[12] The 4D Architecture for Network Control and Management [EB/OL]. [2007-05-08] http://www.cs.cmu.edu/~4D/

[13] Medium and long-term national scientific and technological development program [EB/OL]. [2007-12-18] http://news.xinhuanet.com/politics/2006-02/09/content_4156347.htm (in Chinese)
(国家中长期科学和技术发展规划纲要[EB/OL]. [2007-12-18] http://news.xinhuanet.com/politics/2006-02/09/content_4156347.htm)

[14] Jiang Yixin. From Trusted Computing to Trustworthy Networks [EB/OL]. [2008-08-18] http://media.ccidnet.com/art/2617/20060512/551589_1.html (in Chinese)
(蒋屹新. 从可信计算到可信网络[EB/OL]. [2008-08-18] http://media.ccidnet.com/art/2617/20060512/551589_1.html)

[15] Lin Chuang, Ren Fengyuan. Controllable, trustworthy and scalable new generation Internet[J]. Journal of Software, 2004, 15(12): 1815-1821 (in Chinese)
(林闯, 任丰原. 可控可信可扩展的新一代互联网[J]. 软件学报, 2004, 15(12): 1815-1821)

[16] Tian Liqin, Qiao Anjuan, Lin Chuang, *et al*. Kind of quantitative evaluation of user behavior trust using AHP [J]. Journal of Computational Information Systems, 2007, 3(4): 1329-1334

[17] Lin Chuang, Wang Yang, Li Quanlin. Stochastic modeling and evaluation for network security [J]. Chinese Journal of Computers, 2005, 28(12): 143-156 (in Chinese)
(林闯, 汪洋, 李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005, 28(12): 143-156)

[18] Tian Liqin, Lin Chuang, Ji Tieguo. Quantitative analysis of trust evidence in Internet [C] //Proc of the 10th Int Conf on Communication Technology (ICCT2006). Piscataway, NJ: IEEE, 2006: 194-198

Lin Chuang, born in 1948. Ph. D., professor and Ph. D. supervisor. His current research interests include QoS, performance evaluation, trustworthy network, and Petri net theory together with its applications, etc.
林　闯, 1948年生, 教授, 博士生导师, 主要研究方向为系统性能评价、网络QoS、网络安全计算、随机Petri网等.

Tian Liqin, born in 1970. Associate professor, Ph. D. candidate and master supervisor of the Information Engineering School, Beijing University of Science and Technology. He received his master's degree in the Department of Computer Science and Technology, Tsinghua University in 2003. His current research interests include computer networks, performance evaluation, network security and trustworthy networks.
田立勤, 1970年生, 博士研究生, 副教授, 硕士生导师, 主要研究方向为计算机网络、工作流模型、网络安全和可信网络.

Wang Yuanzhuo, born in 1978. Ph. D. and assistant researcher in Tsinghua University, and senior member of China Computer Federation. His main research interests include trusted network, grid computing, network QoS, security evaluation, *etc*.
王元卓, 1978年生, 博士, 助理研究员, 中国计算机学会高级会员, 主要研究方向为网络QoS、可生存性分析、网络安全、网格计算等.

Research Background

In recent years, the trustworthy network research has become a research focus. An important objective of our projects is to probe the user behavior trust of trustworthy network, which brings the following four benefits for TN. Firstly, behavior trust-based control is more particle size finer, more specific and dynamic than the identity trust-based control. Secondly, the research on the user behavior trust is to strengthen weak links in the TN. We can see that user is weak links in the TN composed of the service providers, users and the network itself. Thirdly, in recent years, experiences in network application show that network security does not indicate the information security of all. Content security is a very important part of the network security. If the content of the information between users can not be guaranteed, even if the network is very secure, information security can not be guaranteed. Fourthly, the study of users behavior trust can predict user behavior in advance before any damage achieves initiative and foresight of control. In this paper, we systematically put forward a framework for evaluation, prediction and control of user behavior trust, which strengthens the dynamic state processing of the user trust, providing the strategy foundation for the implementation of intelligent adaptive network security in the TN.

This research is supported by the National Natural Science Foundation of China (Nos. 90718040, 60872055, 60673187, 60803123), the National Grand Fundamental Research 973 Program of China (No. 2006CB708301), and the Science and Technology Project of Hebei Province (No. 07213570).