线上社交网络访问控制模型综述①

刘 娜, 叶春晓

(重庆大学 计算机学院, 重庆 400044)

摘 要: 就线上社交网络访问控制模型的研究现状进行了分析、总结, 指出当前研究中存在的关键问题和面临的挑战, 并对此类模型的发展趋势和未来研究方向做出预测. 线上社交网络方兴未艾, 数据共享、隐私保护等问题日渐引起公众注意. 作为信息安全手段, 传统访问控制模型已不适应线上社交网络复杂环境下的安全需求. 近年来针对线上社交网络访问控制模型的研究正成为热点问题, 多个研究小组均从不同角度提出了新的访问控制模型.

关键词: 线上社交网络; 访问控制模型; 隐私保护; 策略语言; 策略冲突消解

Survey on Access Control Models for Online Social Networks

LIU Na, YE Chun-Xiao

(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: The research status of access control models for online social networks was analyzed and summarized. The key problems and challenges were also pointed out, and some development trends and future research directions was proposed. Along with the explosive development of online social networks, problems such as data sharing and privacy preservation are gradually grabbing the attention of the public. As information security mechanism, traditional access control models are incompetent to meet the security requirements under the complex circumstances of online social networks. Recent years, research on access control models for online social networks is becoming a hot topic and many new access control models have been proposed based on different perspectives.

Key words: online social networks (OSNs); access control model; privacy preservation; policy language; policy conflicts solution

线上社交网络(OSNs: Online Social Networks)开始成为人们互通有无的平台, 其应用迅速发展到很多方面. 据估测: 到 2014 年互联网用户每月至少一次访问 OSNs 的比例将从 2008 年的 41%上升到 65%[1]. 线上社交网络的隐私保护和信息安全成为人们关心的热点问题[2].

访问控制是实现信息安全的关键策略之一, 但传统集中式访问控制模型已不适应 OSNs 复杂环境下的隐私保护和信息安全需求. 近年来, 国外多个研究小组均从不同角度提出了新的访问控制模型, 以期为 Web2.0 时代蓬勃发展的 OSNs 提供兼顾隐私与效率的信息安全策略. 新模型的研究由于起步较晚, 目前正呈现百花齐放百家争鸣的态势, 尚未形成公认的如传统访问控制的 MAC、DAC、RBAC 式壁垒分明的流派.

同时, 无论国内、国外, 都缺乏 OSNs 访问控制模型研究现状的系统性分析和总结. 尤其在国内对 OSNs 的研究主要集中在其商业应用、舆情监控作用, 或以信任算法、隐私保护方法、路径发现算法为切入点进行的窄面研究, 系统性信息安全方面涉及甚少, 不仅尚未有成型的 OSNs 访问控制模型, 系统全面介绍 OSNs 信息安全解决方案、访问控制模型的调研性综述更是尚属空白.

本文从核心思想、基本技术、策略语言、策略冲突消解方法、优缺点等方面尝试对已提出的 OSNs 访问控制模型进行分类、对比和总结, 指出关键问题和面临的挑战, 并对其发展趋势和未来研究方向做出合

① 收稿时间:2013-10-01;收到修改稿时间:2013-10-25

© 中国科学院软件研究所 http://www.c-s-a.org.cn

理预测, 以便读者能够对 OSNs 访问控制模型的重要概念有个理性的认识, 清晰把握其发展脉络, 理清问题的关键点, 也为读者思考 OSNs 访问控制模型未来发展方向提供一个参考.

1 几个重要概念

1.1 线上社交网络

作为 Web2.0 时代新兴的网络现象, OSNs 并没有一种公认的术语或者广为接受的定义. 比较流行的术语有 Schneider 等提出的 Online Social Network(OSN)[3], 定义为: 在拥有相似爱好、活动、背景、朋友圈的人之间建立的在线社区, 多数基于 Web, 允许用户上传个人资料, 以多种方式互动. 此定义涵盖了用户和资源两个方面. Boyd 提出的 Social Network Site(SNS)[4], 定义为: 基于 Web 的服务, 允许用户在一定范围的系统内构建公开或半公开个人资料, 可与其它用户建立连接, 并在系统内部共享、传递连接列表. 此定义面向用户, 突出用户在 OSNs 中的主导地位. 还有 Adamic 提出的 Social Networking Service(SNS)[5], 定义为: 聚集用户社交联系人信息, 构建庞大的内部互联的社交网络, 为用户揭示怎样在网络中联系他人的服务. 此定义着重突出社交网络构建过程和服务性质.

本文讨论的 OSNs 比较接近 Schneider 的定义, 但所指范围有所扩大, 同时包含用户、资源和活动三个方面, 不止是小圈子内建立的在线社区, 而是基于 Web, 任何人均可加入, 提供多种网络社交服务, 用户可对个人信息和他人发布资源进行多种操作的综合性线上社交服务站点.

1.2 隐私保护

OSNs 用户可以自由发布个人信息, 这种自由性导致各种意想不到的隐私威胁. Zheleva[6]揭示了 OSNs 中的 4 种隐私问题: 身份、属性、社会关系和组关系. 身份即为现实世界中用户的真实身份. 属性包括身份证号、姓名、住址、政治倾向、性向等标识一个人特征的东西. 社会关系包括朋友、亲属、亲密联系人等. 组关系则是用户加入的兴趣小组、圈子、讨论组等. 4 种隐私问题均属于与用户切身相关的敏感信息, 若保护不周, 极有可能被窃取用于诈骗、保险欺诈等违法犯罪行为.

前几年对敏感属性暴露问题已有一些研究, 但大多关注点在如何预测属性, 而非如何保护. 近几年国外的研究集中在对用户隐私评估和个性化制定个人隐私策略上. 国内偏重信任算法、匿名化方法、节点发现算法等[7-9]隐私保护类算法的研究. 但现有 OSNs 的安全措施对个人信息的访问控制不很完善, 就算用户设置了对某些访问进行限制, 有心人往往可以从别的地方(如: 朋友、社区、圈子)获取到用户想屏蔽的个人信息[10]. 隐私保护是 OSNs 安全策略中绕不开的问题, 也是 OSNs 访问控制模型设计与实现中必须考虑的问题.

1.3 策略语言

访问控制策略语言的选择范围较广, 既可以应用发展成熟的正则表达式、四值逻辑等, 也可以结合新兴的语义网技术, 或者融合多种逻辑语言形成自成体系的策略语言.

Carminati[11]认为 OSNs 用户互动方式复杂, 用户和资源间也有多种访问方式, 策略语言应该做到: 1)基于关系: U2U(User-to-User)是考虑重点, 且由于路径深度、信任级别没有必然联系, 策略语言除了要能表达对路径深度的限制还要支持对关系上最低信任级别的限制; 2)U2R(User-to-Resource) 、 R2R(Resource-to-Resource)也必须考虑进去: 如某用户是一些资源的拥有者同时也被其它用户在相册里做了标记, 这种时候策略语言要能表达 OSNs 支持的多种 U2R、R2R 关系.

2 分类体系

OSNs 访问控制模型研究正处于新兴阶段, 没有已成型的通用理论. 在 OSNs 访问控制模型研究早期, 受信任和信誉系统启发, 出现了一系列基于信任的访问控制模型. 其中的典型代表是 Kruk 等提出的 D-FOAF[12]和 Carminati 等提出的基于规则的访问控制模型[13,14]和分布式安全框架[15].

Carminati 等人随后基于语义网技术应用网页本体语言(OWL: Web Ontology Language[1])和语义网规则语言(SWRL: Semantic Web Rule Language)提出 OSNs 访问控制框架[16]并产生了原型实现[17]. 与之类似的, 基于本体的 OSNs 访问控制模型还有 Masoumzadeh 提出的 OSNAC[18].

Fong 等人于 2009 年首先对 Facebook 隐私保护机制

[1] OWL 是 W3C 开发的一种网络本体语言, 用于对本体进行语义描述. http://www.w3.org/TR/owl-ref/

© 中国科学院软件研究所 http://www.c-s-a.org.cn

背后的访问控制规范做了形式化描述, 使用基于拓扑的访问控制策略形成类 Facebook 系统隐私保护模型[19], 并持续对此模型进行扩展, 形成基于关系的 OSNs 访问控制模型 ReBAC[20-22].

Park 等人领导的研究小组认为 OSNs 的访问控制更多地由基于社会关系图的用户关系网驱动, 在 2011 年从用户活动角度描述了一种 OSNs 的访问控制框架[23], 随后提出基于 U2U 关系的访问控制模型[24], 在此基础上引入 U2R、R2R 关系, 形成更完善的基于关系的 OSNs 访问控制模型[25].

此外, OSNs 访问控制模型不可或缺的策略语言, 策略组合方法, 加密数据共享, 多方授权, 策略冲突检测与消解等问题也有研究小组进行过探讨.

从核心思想、基本技术、特性、性能出发, 可将主流 OSNs 访问控制模型分为表 1 所示的几种类型.

表 1 OSNs 访问控制模型分类

类型	核心思想	基本技术	特性	性能	典型代表
基于信任	以关系类型、信任级别、路径深度聚合的信任值为授权依据	分布式身份管理、授权委托、信任计算	授权依据确定, 规则制定简单	信任值计算效率低, 扩展性不佳	[11]、[12]、[13]
基于语义网	语义网技术展现用户与资源间的多种关系	语义网、OWL、SWRL、本体	符合资源共享需求, 细粒度, 可扩展	首次加载时间过长, 规则推导效率低	[16]、[17]
基于关系	形式化表达社交图谱拓扑中多种关系, 以关系类型、深度定义授权策略	模态逻辑、混合逻辑、正则表达式、路径检查算法、冲突消解	策略个性化, 支持多关系, 细粒度, 授权灵活, 表达能力强	准确性高, 搜索效率稳定, 具简单冲突消解能力	[19]、[20]、[21]、[23]、[24]

3 发展脉络与研究现状

3.1 基于信任的 OSNs 访问控制模型

Kruk 和 Carminati 受信任和信誉系统启发, 基于资源拥有者和请求者间的关系类型、信任级别、关系路径深度聚合信任值, 并将此信任值作为授权的参数之一, 提出了基于信任的 OSNs 访问控制模型.

Kruk 的 D-FOAF[11]系统是基于本体的分布式身份管理系统, 展示了社交网络中信息继承用于社区驱动的访问权限委托, 并分析了分布式身份管理、授权和访问权限检查算法. 但此系统只考虑了“朋友的朋友”一种关系类型, 未涉及 U2R 和 R2R 关系. 对功能愈加繁复的 OSNs 来说显然不足够.

而 Carminati 的模型[12]在概念上与 Kruk 类似, 都是基于信任. 他利用证书保障关系的真实性, 以基于规则的方式在用户端实现访问控制. 允许有多种关系类型, 资源间也可指定访问规则, 只是在计算关系路径的信任值时一次只允许一种类型.

在半自主架构的访问控制实现方案[13]中, 个人用户可以自主方式用关系类型、深度和信任矩阵在用户端设置访问规则, 资源请求者必须向被请求者提供证据证明自己是被授权的. 此方案特点在于关系路径有效性认证为可信证书服务器集中式管理而访问控制策略由分散的用户端制定.

OSNs 访问控制的实现理论上非集中式最佳, 这可避免传统上完全委托给社交网络管理系统集中进行授权所可能造成的信息安全问题(系统并非一直那么诚实和透明, Facebook 某些服务收集和发布用户数据的行为就被发现过[10]). 但若完全分散式实现, 那信任值计算任务可能会非常难以实施且很耗时间. 分布式身份管理采用本地缓存保留权限计算时可能会用到的节点间路径以提高计算效率, 半自主架构可平衡信任计算效率与策略弹性问题.

基于信任的访问控制模型应用于 OSNs 环境仿佛是很自然的事, 但信任值计算却难以在兼顾效率与隐私安全的情况下实现. 由信任值作为主要参数决定访问控制规则也尚未涵盖 OSNs 复杂的 U2U、U2R、R2R 关系. 相对于后来出现的基于语义网技术和基于关系的访问控制模型, 基于信任的模型在对 OSNs 复杂社交图谱的刻画上显得过于薄弱, 访问控制管理也略显生硬, 扩展性不佳. 此类模型中留有两个开放性问题[26]: 第一, 当信任用于可控信息分享时, 信任的语义是什么? 第二, 在 OSNs 动态、复杂的环境下, 信任该如何计算, 怎样监控?

3.2 基于语义网技术的 OSNs 访问控制模型

语义网是由 Tim Berners-Lee 于 1998 年提出的概念. 旨在通过给全球信息网上的文档添加能被计算机理解的语义, 使之成为一个通用的信息交换媒介.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

Carminati 于 2009 年提出基于语义网的社交网络访问控制框架[15], 将语义网技术引入 OSNs 访问控制, 随后提出基于语义网的访问控制模型[16], 用语义网本体刻画社交网络相关信息, 对5个OSNs的重要方面建模: 1)用户个人信息; 2)用户间关系; 3)资源; 4)用户-资源间关系; 5)行为. 此模型定义了三种访问策略: 授权、管理和过滤, 展现了用户与资源间的多种关系, 符合 OSNs 环境下 U2R 关系多样化的趋势. 访问控制策略在本体基础上由 SWRL 规则表达, 是可扩展、细粒度的访问控制模型. 但缺乏形式化描述, 实现也很模糊. 只用 JENA[2] 实现了原型系统, 且只在自己产生的数据集上做了测试, 没有用真实的OSNs数据. 实验结果也表明此模型加载时间过长, 对内存空间要求过大, 效率尚有改进余地. 不过, 随着用户的朋友数增加而应用访问控制规则的时间倒只是线性增长.

Masoumzadeh 同样受语义网技术启发, 于2010年使用社交网络系统本体 SNO(Social Network system Ontology)描述信息语义, 提出访问控制本体 ACO (Access Control Ontology)概念和基于本体的社交网络访问控制模型 OSNAC[17], 并提供了访问控制引擎的实现. 此模型使用ACO和策略强调对知识库中语义丰富的信息的保护. 其策略将规则分为用户层和系统层. 用户层可以委托、依赖和多方决策等方式来提高灵活性. 用户和系统都有更细粒度的访问控制策略. 但本体和规则推导的效率及本体数据和每条策略组件的引入而产生的复杂性问题需引起研究人员的注意.

3.3 基于关系的 OSNs 访问控制模型

Web2.0 时代对访问控制提出的要求中最重要的一点就是要可以像在现实世界一样根据接收者本体来控制信息流向, 而不是基于接受者的角色来控制[27]. 达到这一要求最自然的方式就是基于社交图谱关系来构建访问控制模型.

2009年, Fong等人分析了Facebook的访问控制机制, 将其隐私保护机制背后的访问控制规范形式化为访问控制模型[18]. 这是首个基于实际 OSNs 抽象出的访问控制模型, 抓住了OSNs基于关系的特征. 虽然其策略在实际系统中并未有采用的迹象, 但为后面进行基于关系的 OSNs 访问控制研究提供了借鉴.

随后他以 U2U 关系为核心, 引入模态逻辑语言, 提出了形式化的基于关系的访问控制模型 ReBAC[19]. 此模型引入了策略制定语言, 但表达能力尚须增强, 某些关系类型表达不出, 由此也引发了对 OSNs 访问控制策略语言的探讨. 之后, 此模态逻辑语言被扩展, 增强了语言的表达能力[20], 使 ReBAC 支持多关系和方向性关系, 以及上下文中的关系共享, 为策略语言研究打开了一扇窗. 但模态逻辑语言本身并不能表达某些关系. 对子策略的评估、从关系图方程中有效率地计算出策略决策的能力也欠缺.

Bruns 使用混合逻辑(Hybrid Logic)[21]改进 ReBAC, 提高了策略评估效率和原子公式的灵活性. 在基于关系的访问控制策略制定上, 混合逻辑比模态逻辑的表达能力更强, 效率更高.

OSNs 的访问控制更多地由基于社会关系图的用户关系网驱动. Park 等人从用户-活动角度描述了一种适应 OSNs 的访问控制框架[22], 与传统框架不同之处在于除了能使用户对普通活动进行访问控制之外, 也可对用户的控制活动进行控制. 此框架特色: 1)策略个性化: 每个用户均可设定自己的策略, 用户个人或其相关者都可以自己维护策略. 2)用户和资源分离, 支持用户会话. 此框架为未来支持更强的安全与隐私保护的 OSNs 访问控制模型研究奠定了基础. 但策略个性化也引入了策略冲突问题.

U2U 关系是 OSNs 结构的基础, Cheng 等人在之前的框架下基于 U2U 关系, 以正则表达式作为策略语言, 运用基于深度优先搜索的路径检查算法, 提出了基于用户间关系的访问控制模型 UURAC[23]. 此模型只有 U2U 关系, 未包含 U2R、R2R 关系, 一对多关系也未刻画. 正则表达式作为策略语言表达清晰但表达能力尚有不足, 深度优先搜索算法发展成熟, 可保证准确性.

在 UURAC 基础上, 引入 U2R、R2R 关系, 调整授权策略, 并提供简单的冲突消解策略, 完善了 UURAC 模型[24]. 其授权策略由路径类型和用户间关系路径跳数定义而忽略资源相关的路径跳数, 比较灵活, 表达能力更强. 有相对简单的冲突消解能力, 未涉及对多方授权的描述.

3.4 其它相关研究

Bruns 基于 Belnap 的四值逻辑提出策略语言 PBel[28], 将访问请求分为允许、拒绝、冲突和空白, 很

[2] 开源语义网应用开发框架 http://jena.sourceforge.net/.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

好地涵盖了策略语言需求: 支持策略制订; 既有访问权也有限制权; 能通过静态分析检测策略冲突和空白; 支持抽象层, 既能封装具体结构系统也能跨应用跨系统. PBel 的提出为 OSNs 访问控制策略语言提供了一种选择, 但是否必须由四值逻辑实现尚有待考察.

XACML 是早已应用的访问控制规则制订和组合工具, 但其缺乏形式化语义, 会导致计划外的决策组合和不恰当的策略决策评估. Ni 为了在访问控制领域对决策建模, 提出一种决策形式化体系: D-algebra[29]. 希望它作为比 XACML 更好的访问控制策略组合工具, 但并未给出具体应用, 实际效果如何尚待验证.

Shuai 采用基于属性加密的 ABE 访问控制机制为 OSNs 中加密数据的互动分享提供了一种层次性的解决方案 Masque[30]. 此方案使用 7 个算法, 允许 OSNs 提供商在高层级管理用户而不触及他们的敏感数据, 同时允许用户定制个性化的访问策略. 但如何实时撤销以使用户可以灵活重定义访问策略尚有待解决, 加解密效率在用户数量很大、加解密需求频繁的时候如何保证也是个问题.

OSNs 中用户不仅可以自己上传资源, 还可以标记他人资源或者在他人空间里发布评论、粘贴照片. 这些共享信息涉及到多名用户, 而多数 OSNs 访问控制模型只允许资源拥有者制定访问策略, 未考虑到其他如数据贡献者、利益相关者和传播者等对共享资源访问控制的诉求. Hu 提出 MAF (Multiparty Authorization Framework)[31], 用多方策略制定方案和相应的策略评估机制, 对多方授权问题进行建模, 并实现了一个基于 Facebook 的第三方应用 MController 以展示 MAF 模型和机制的特性. 其多方隐私冲突解决方案采用基于投票的弹性机制, 决策投票和敏感性投票相结合, 兼顾隐私保护和系统可用性.

4 问题和挑战

OSNs 社交图谱复杂, 隐私保护和信息安全需求都与以往访问控制模型面对的单一系统不同, OSNs 环境下的访问控制是一个新兴领域, 面临许多问题和挑战.

首先, 策略冲突检测与解决问题. OSNs 环境下, 每个用户都应能参与访问控制策略制定, 用户与系统本身共同承担安全与隐私维护. 当多个用户对同一资源的访问策略产生冲突, 或用户自定义的访问策略与系统基础策略冲突时, 如何取舍? 怎样决策?

现有模型中采取的解决方案或由系统收集各用户策略权衡采用, 或以用户间关系路径跳数决定其策略优先级. 用户个性化设定再由系统取舍的方案其本质尚未摆脱单一系统集中式管理的模式, 灵活性不足; 且策略若要变更则牵涉甚广, 系统开销大. 若由关系路径跳数决定资源访问策略的优先级则又忽略了资源拥有者、直接关系者、贡献者等对资源访问策略的控制权, 且关系路径跳数未必能真实反映请求者与被请求资源间关系的紧密度(如照片中出现的人可能对照片拥有者而言是路人, 却正好是访问请求者本人).

策略冲突消解问题在多个模型中都有提到, 但仍属开放性问题, 尚未有既切实有效又易于实施, 系统开销小, 能满足多个用户和系统本身对策略执行和调整灵活性的要求的.

其次, 准确性与效率问题. 每次访问请求的决策要考虑到请求者与所访问资源、资源拥有者、利益相关者和传播者多方的关系类型、信任级别、关系路径深度、各自授权策略等. 决策相关数据的产生、比较、聚合、存储和最终决策都可能带来系统开销上的巨大负担.

尽管自基于信任的访问控制模型提出以来就有各种信任值计算算法、关系路径搜索算法、加解密算法等被应用到授权策略准确性的保证上来, 也有诸如设立策略缓存, 子策略评估等措施来一定程度上提高访问控制策略实施的效率. 但在 OSNs 动态、复杂的环境下, 对准确性和效率的要求只会越来越高, 对已有算法、机制的增删整合或者独辟蹊径引入新机制在保证决策准确合理的同时兼顾效率, 是 OSNs 访问控制模型研究者无法回避的问题.

再次, 隐私泄露的挑战. OSNs 的访问控制更多地由基于社会关系图的用户关系网驱动, 其实现必然在一定程度上会暴露部分关系. 高效通用的私有路径发现方法尚处于开放性问题. Jin 等人就曾用 MFB (Mutual-Friend Based)攻击技术[32], 在 Facebook 离线数据集上通过暴露的朋友和附近邻居节点, 成功获取攻击目标的部分甚至整个社会关系图. 怎样避免非必要的隐私泄露是 OSNs 访问控制面临的一大挑战.

此外, 在计算信任级别时也可能会暴露隐私, 比如需要两者间的互动记录等等. 如何准确高效、隐私安全地计算信任值也有待研究.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

5 发展趋势与研究方向

OSNs 社交关系图谱庞大, 基于关系的访问控制模型更有利于表达其中复杂的各种关系, 构建拥有丰富、自然的社会意义的访问控制策略组合. 因而, OSNs 访问控制模型的发展趋势可能会以基于关系的为主, 融合信任值计算与本体技术, 力求详实、自然地覆盖 OSNs 社会关系图谱和基于其上的行为.

访问控制策略个性化是 OSNs 的内在要求, 需要有较强表达能力的策略语言, 授权策略需灵活, 有一定冲突检测和消解能力. 已有的策略语言, 如: OWL、SWRL、模态逻辑语言、混合逻辑、正则表达式、基于四值逻辑的 PBel 语言等, 要么表达能力较差, 要么规则推导效率较低, 要么缺乏策略冲突检测与解决能力. OSNs 访问控制模型研究中一个重要研究方向可能是表达能力强、效率高、具备冲突检测与消解能力的访问控制策略语言. 可以考虑走融合改进已有策略语言路线.

访问决策过程中涉及到的路径搜索、信任值计算等算法和决策机制必须准确而有效率. 由于模式识别技术的发展, 从相片等内容中准确识别身份并自动产生标记的算法也会出现, 隐私相关的访问控制在将来会更为复杂, 需要发展更为尖端有效的解决方案以应对 OSNs 中多种共享数据的安全与隐私挑战. 其中势必涉及到加解密算法、密钥分配方案等的研究.

策略管理是另一大研究方向, 因为 OSN 社交图谱很大且随时处于变化中, 用户需要非常灵活的策略语言来表达他们的隐私需求, 需要有效的技术和工具来评估非授权信息流的风险.

综合以上分析, 未来 OSNs 访问控制模型仍会以基于关系为主流, 研究方向可能集中在策略语言开发、高效通用的路径发现算法、多方授权和策略冲突解决方案、隐私泄露风险评估、策略管理等方面.

6 结语

本文对线上社交网络访问控制模型的研究现状进行了分析和对比, 给出模型分类体系, 描绘出清晰的发展脉络. 通过分析总结, 指出 OSNs 访问控制研究关键点在于社会关系图谱表达、策略冲突消解、决策准确性和效率, 以及隐私泄露问题, 并由此提出 OSNs 访问控制模型的发展趋势仍会以基于关系为主, 未来研究重点可能在策略语言、路径发现算法、多方授权和策略冲突解决方案, 隐私泄露风险评估和策略管理.

参考文献

1 Heideman J, Mathias K, Probst F. Online social networks: a survey of a global phenomenon. Computer Networks, 2012, 56(18): 3866–3878.

2 Mo MZ, King I, Leung KS. Empirical comparisons of attack and protection algorithms for online social networks. Procedia Computer Science, 2011, 5: 705–712.

3 Schneider F, Feldmann A, Krishnamurthy B, et al. Understanding online social network usage from a network perspective. Proc. of the ACM SIGCOMM Conference on Internet Measurement. 2009. 35–48.

4 Boyd DM, Ellison NB. Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication, 2007, 13(1): 210–230.

5 Adamic LA, Adar E. How to search a social network. Social Networks, 2005, 27(3): 187–203.

6 Zheleva E, Getoor L. Privacy in social networks: a survey. Social Network Data Analytics. US, Springer US. 2011. 277–306.

7 Bao J, Cheng JJ. Group trust algorithm based on social network. Computer Science, 2012, 39(2): 38–41, 51.

8 Wei W, Li Y, Zhang WQ. Study on GSNPP algorithm based privacy-preserving approach in social networks. Computer Science, 2012, 39(3): 104–106.

9 Wang XG. Discovering critical nodes in social networks based on cooperative games. Computer Science, 2013, 40(4): 155–159.

10 Ajami R, Ramadan N, Mohamed N, et al. Security challenges and approaches in online social networks:a survey. International Journal of Computer Science and Network Security, 2011, 11(8): 1–12.

11 Carminati B, Ferrari E. Privacy-aware access control in social networks: issues and solutions. Privacy and Anonymity in Information Management Systems, Advanced Information and Knowledge Processing. London, Springer-Verlag London Limited. 2010. 181–195.

12 Kruk S, Grzonkowski S, Gzella A et al. D-FOAF: Distributed identity management with access rights delegation. Semantic Web- ASWC 2006 Proceedings. Berlin Heidelberg. Springer-Verlag, Berlin Heidelberg. 2006. 140–154.

13 Carminati B, Ferrari E, Perego A. Rule-based access control

© 中国科学院软件研究所 http://www.c-s-a.org.cn

for social networks. In: Meerman R,Tari Z, Herrero P, eds. On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Berlin Heidelberg. Springer Berlin Heidelberg. 2006. 1734−1744.

14 Carminati B, Ferrari E, Perego A. Enforcing access control in web-based social networks. ACM Transactions on Information and System Security, 2009, 13(1): 1−38.

15 Carminati B, Ferrari E, Perego A. A decentralized security framework for web-based social networks. International Journal of Information Security and Privacy, 2008, 2(4): 22−53.

16 Carminati B, Ferrari E, Heatherly R, et al. A semantic web based framework for social network access control. SACMAT'09, Proc. of the 14th ACM Symposium on Access Control Models and Technologies. NY, USA. ACM New York. 2009. 177−186.

17 Carminati B, Ferrari E, Heatherly R, et al. Semantic web-based social network access control. COMPUTERS & SECURITY, 2011, 30(2-3): 108−115.

18 Masoumzadeh A, Joshi J. OSNAC: an ontology-based access control model for social networking systems. SOCIALCOM'10, Proc. of the 2010 IEEE Second International Conference on Social Computing. Washington DC, USA. IEEE Computer Society. 2010. 751−759.

19 Fong PWL, Anwar M, Zhao Z. A privacy preservation model for Facebook-Style social network systems. In: Michael B, Peng N, eds. Computer Security-ESORICS 2009, 14th European Symposium on Research in Computer Security. Saint-Malo, France. September 21-23, 2009. Berlin Heidelberg. Springer-Verlag. 2009. 303−320.

20 Fong PWL. Relationship-based access control: protection model and policy language. CODASPY'11, Proc. of the first ACM Conference on Data and Application Security and Privacy. NY, USA. ACM New York. 2011. 191−202.

21 Fong PWL, Siahaan I. Relationship-based access control policies and their policy languages. SACMAT'11, Proc. of the 16th ACM Symposium on Access Control Models and Technologies. NY, USA. ACM New York. 2011. 51−60.

22 Bruns G, Fong PWL, Siahaan I, et al. Relationship-based access control: its expression and enforcement through hybrid logic. CODASPY'12, Proc. of the second ACM Conference on Data and Application Security and Privacy. NY, USA. ACM New York. 2012. 117−124.

23 Park J, Sandhu R, Cheng Y. A user-activity-centric framework for access control in online social networks. IEEE Internet Computing, 2011, 15(5): 62−65.

24 Cheng Y, Park J, Sandhu R. A user-to-user relationship-based access control model for online social networks. Data and Applications Security and Privacy XXVI. Berlin. Springer Berlin Heidelberg. 2012. 8−24.

25 Cheng Y, Park J, Sandhu R. Relationship-based access control for online social networks: beyond user-to-user relationships. Proc. of 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust(PASSAT). Amsterdam. IEEE Computer Society. 2012. 646−655.

26 Ferrari E. Access control, privacy and trust in on-line social networks: issues and solutions. In: Nicola BM, Giuseppe B, Luca S, eds. Trustworthy Internet. Springer Milan. 2011. 203− 212.

27 Gates CE. Access control requirements for Web 2.0 security and privacy. W2SP'07, Proc. of IEEE Web2.0 Securityand Privacy Workshop. Oakland, California. May 2007.

28 Bruns G, Huth M. Access control via belnap logic: Intuitive, expressive, and analyzable policy composition. ACM Trans. on Information and System Security, 2011, 14(1): Article 9.

29 Ni Q, Bertino E, Lobo J. D-algebra for composing access control policy decisions. Proc. of the 4th International Symposium on Information, Computer, and Communications Security. NY, USA. ACM. 2009. 298−309.

30 Shusai H, Zhu WT. Masque: access control for interactive sharing of encrypted data in social networks. In: Xu L, Bertino E, Mu Y, eds. Network and System Security. Berlin Heidelberg. Springer-Verlag. 2012. 503−515.

31 Hu H, Ahn GJ. Multiparty authorization framework for data sharing in online social networks. In: Li Y, ed. Data and Applications Security and Privacy XXV. Berlin Heidelberg. Springer. 2011. 29−43.

32 Jin L, Joshi J, Anwar M. Mutual-friend Based Attacks in Social Network Systems. Computers & Security, 2013. 10.1016 / j.cose.2013.04.003.

© 中国科学院软件研究所 http://www.c-s-a.org.cn