

面向社交网络的访问控制模型和策略研究进展

陈天柱, 郭云川, 牛犇, 李风华

(中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093)

摘要: 作为信息保护有效手段之一的访问控制技术, 可以保障信息仅能被合法用户访问, 防止信息的泄露, 势必成为在线社交网络中信息保护方法的重要组成部分。通过分析在线社交网络的特点, 从访问控制模型与访问控制策略 2 个角度出发, 对目前在线社交网络中的访问控制研究进行深入探讨, 并对相关研究进行整理与分析。

关键词: 社交网络; 访问控制模型; 访问控制策略; 信息传播

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00086

Research progress of access control model and policy in online social networks

CHEN Tian-zhu, GUO Yun-chuan, NIU Ben, LI Feng-hua

(State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: As one of the effective approach to protecting information, access control which makes the information only accessed by legitimate users and prevents information leakage, has been widely used in online social networks. The characteristics of OSN were analyzed. From two angles of access control model and access control strategy, the research of access control in online social networks were discussed deeply, the related research was counted and analyzed.

Key words: social network, access control model, access control policy, information dissemination

1 引言

近年来在线社交网络 (OSN, online social network) 不断发展, 已成为人们日常生活中必不可少的组成部分。用户在社交网络上分享消息以便和朋友、同事、同学甚至是陌生人之间相互交流。据统计, 每天 Twitter 上的用户会分享 5 亿条信息, Instagram 上的用户会分享 6 000 万张图片

信息^[1]。用户的交流信息、配置信息、分享的图片信息等含有大量的敏感信息, 这些信息的泄露和不正常传播会给用户带来极大的隐私隐患。为缓解用户的隐私忧虑, 大部分社交网络都采取了对信息的访问控制策略, 并且将访问控制策略描述、执行权限赋予用户本身。Facebook 允许用户对每个信息制定不同的访问控制权限, Twitter 和 Instagram 为用户提供了更加细粒度的访问控制策略。

收稿日期: 2016-05-26; 修回日期: 2016-07-12。通信作者: 李风华, lfh@iie.ac.cn

基金项目: 国家高技术研究发展计划 (“863”计划) 基金资助项目 (No.2015AA016007); 国家自然科学基金委—广东联合基金资助项目 (No.U1401251); 国家科技重大专项基金资助项目 (No.2015ZX01029101)

Foundation Items: The National High Technology R&D Program of China (863 Program) (No.2015AA016007), The National Natural Science Foundation of China-Guangdong Union Foundation (No.U1401251), The National Science and Technology Major Project of China (No.2015ZX01029101)

OSN 具有和传统系统不同的特点, 具体来说, 社交网络为每个用户提供一个虚拟空间, 此虚拟空间上存有朋友列表、交流信息、分享信息、评价信息、配置信息、历史信息等。朋友列表显示有大量可使用的控制信息, 这些控制信息对访问控制策略的设计有极大的帮助; 交流信息、分享信息的属性信息能够精确描述一类用户的某些特点从而带来大量的控制信息; 评论信息牵涉到多方用户; 配置信息显示了用户的基本情况, 也提供大量的控制信息; 历史信息显示了用户对朋友的隐私倾向性。

此外, 社交网络还具有以下特点。1) 数据大量性并且极具个人特性。社交网络中的每个用户与朋友不断交流, 产生了大量的信息, 这些信息都是以某些交流话题为中心, 从而显示了用户个人特性。这些信息主要包括朋友之间的交流信息、评论信息、朋友上传的音频信息和视频信息、图片信息等。2) 数据的动态性。社交网络的用户不断分享信息、删除信息, 同时朋友们不断评论信息等, 这使访问客体不断变化。同时访问者可以在不同的地点、不定的时间进行访问, 朋友访问权限的动态性变化等。3) 强隐私性。社交网络上

分享数据的目的是进行相互交流, 从而牵涉到大量的私人信息, 这些数据带有强烈的个人敏感性。

但相关研究结果显示, 大量的 OSN 用户并未对其隐私数据进行保护。例如, 文献[1]通过分析 15 万个 Twitter 用户和 28 万个 Instagram 用户访问控制的使用情况发现, Twitter 用户中设置相应访问控制策略的仅占全部用户的 5.22%, 而在 Instagram 中这一比例也仅为 11.92%。导致用户设置访问控制策略比例如此低的原因在于目前针对 OSN 的访问控制模型和策略不能真实反映 OSN 的特点, 无法满足用户对其数据安全保护的需求。

针对上述提出的 OSN 的复杂环境以及访问控制使用率不高的情况, 加上访问控制在社交网络上数据保护非常重要等原因, 本文对社交网络中的访问控制进行归纳研究, 了解现有社交网络上访问控制模型的优点和缺点、适应情况、解决的问题、使用的技术方法, 以便于未来能够优化并且提出更加适用于社交网络特点模型。

2 面向社交网络的访问控制体系结构

如图 1 所示, 面向社交网络的访问控制模型主要由 3 部分组成: 1) 策略管理点 (PAP, policy

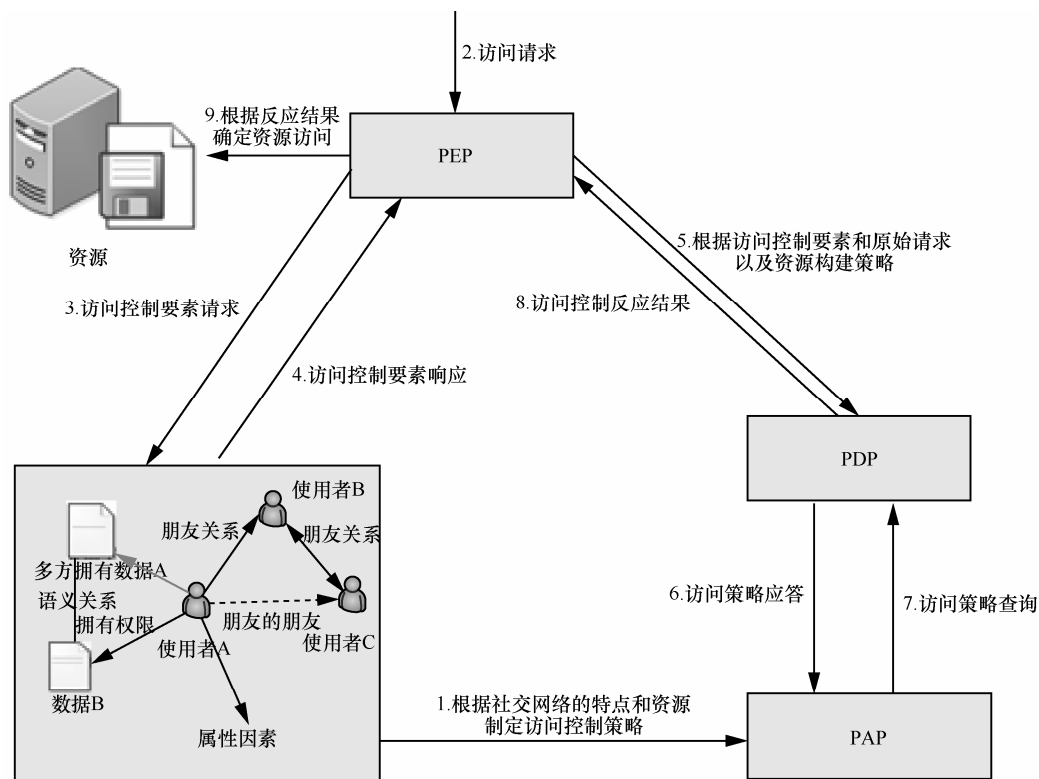


图 1 社交网络中的访问控制体系结构

administration point); 2) 策略实施点(PEP, policy enforcement point); 3) 策略决策点(PDP, policy decision point)。PAP 结合社交网络中控制信息的特点(如用户与朋友之间的关系、关系的复合、朋友之间的信任因素,资源之间的语义关系、资源和用户之间的语义关系、多方信息、配置信息、属性因素、上下文因素等)和访问资源的特点构建相应的访问控制策略。访问者向 PEP 发出针对某个资源的访问请求, PEP 从用户的社交网络结构和对应访问资源的特点中查询访问者的相关控制信息,并将这些对应的控制信息反馈给 PEP, PEP 使用这些反馈信息连同访问的资源、操作方式做出一个访问控制策略,将此策略传递给策略决策点, PDP 询问 PAP 关于此访问者是否具有相关的访问控制权限,并将最终的结果返回给 PEP,最后确定访问者对资源的访问控制权限。

3 面向 OSN 的访问控制模型

3.1 基于关系的访问控制模型

社交网络可抽象为由不同用户及对应社交关系所组成的网络拓扑。在社交网络中,可根据社交关系的类型、深度和可信度等因素对访问者进行细粒度区分,从而精确描述对某一资源的不同权限的访问者。

文献[2]首次将关系(relation)的概念用于访问控制策略管理方面。之后,文献[3]使用直接关系对访问控制策略进行描述。但单纯采用直接关系描述访问控制策略限制了数据的分享,灵活性较差。针对此问题,文献[4]中的模型考虑了直接关系、间接关系,通过对社交网络结构的抽象,提出针对 Facebook 的访问控制模型,加强了 Facebook 对用户数据的分享,此模型不仅对 Facebook 中的访问控制模型进行深刻讨论,解决了关系变化过程中带来的隐私隐患,而且将这个模型广义化应用到与 Facebook 相似的社交网络环境中。

上述基于关系的访问控制模型对关系的强度不加区分,即不对相同跳数的朋友进行区分。但实际应用环境中,不同朋友间的社交关系存在强弱、远近之分,这种不加区分性无法反映出真实的社交关系。针对这一问题,研究者们提出了各

种各样的改进方法。例如,文献[5]通过引入用户间信任度的概念,提出基于信任的访问控制模型;文献[6]提出仿射距离的概念并将其作为可信距离,根据可信距离解决关系强度区分问题,此仿射距离是使用跳数距离和实验数据进行计算。

研究者们通过考虑上述的用户关系类别、用户可信度和朋友深度 3 个因素提出更加细粒度的访问控制模型。例如,文献[7]提出一种基于多关系要素的访问控制模型;文献[8]在用户关系的基础上加入用户—资源及资源—资源间关系,对关系的因素进行扩展,提出一种更为灵活、表达能力更强的访问控制模型。

除了在社交网络中得到广泛应用外,基于关系的访问控制模型在其他应用场景下也得到了应用。文献[9]将基于关系的访问控制模型发展为一种通用的访问控制范例。文献[10]针对文献[9]所提出的表达策略不完全的问题,提出 2 种策略语言的扩展模式并证明了其完整性。文献[11]将文献[9]所提出的通用模型应用到医疗病例系统,解决了传统基于角色医疗病例系统不够精细的问题。

基于关系访问控制的研究从单要素关系类型出发,逐步发展为基于多要素关系类型的访问控制。并在此基础上将关系同其他控制因素相结合,提出许多访问控制模型,如表 1 所示。但这些访问控制模型没有考虑资源的内容和其他因素,不能完全体现出社交网络结构中主体、客体之间的精确关系。因此,增加其他因素使其能够更加精细地识别每个访问者的身份,是社交网络访问控制研究的重点之一。

3.2 基于属性的访问控制模型

社交网络具有动态性,用户可随时随地添加/删除好友、分享/删除各式各样的数据等。属性作为资源的固有因素,可有效对用户、资源、访问者之间的限制条件进行描述。因此,基于属性的访问控制模型^[12~14]适应于具有动态特征的社交网络。

属性因素作为控制因素可有效区分用户的身份、增加更多的约束条件、提出复杂的限制因素,基于这些特征,研究者提出细粒度的访问控制模型。例如,文献[15]针对弱登录证书问题,通过验证登录者的位置属性和证书之间的匹配问题确定其是否具有访问权限,某种程度上保护了被盗

表 1

基于关系的访问控制模型的发展过程

发展历程	控制因素	适用情况	访问控制粒度	存在冲突消解	分散式管理	具有动态性
文献[2, 3]	拥有者和访问者的深度 (1 跳数)	社交网络	不灵活	否	否	否
文献[4]	拥有者和访问者的深度 (多跳数)	社交网络	不灵活	否	是	是
文献[5, 6]	拥有者和访问者的可信级别	社交网络	比较灵活	否	是	是
文献[7]	拥有者和访问者的关系类别、深度 (多跳数)、可信级别	社交网络	比较灵活	否	是	是
文献[8]	拥有者和访问者的关系类别、深度 (多跳数)、可信级别, 资源间的关系	社交网络	灵活	否	是	是
文献 [9, 10]	拥有者和访问者的深度 (多跳数)	和社交网络相似的情景	比较灵活	否	否	是
文献[11]	拥有者和访问者的深度 (1 跳数)	医疗系统	灵活	否	否	是

证书的安全性。文献[16]在基于关系的访问控制策略上增加用户的属性因素, 提出一种细粒度的访问控制模型。文献[17]通过使用角色因素作为限制条件, 提出一个策略自动描述、细粒度的访问控制模型, 这里角色是属性的一个具体实例。文献[18]将公共消息的属性因素作为访问者的附加背景, 增加了用户的限制条件, 并与关系因素相结合定义了新的访问控制模型。信誉是一个团体对一个用户的整体评价, 是一种属性因素。文献[5]利用信誉属性作为限制条件确定访问者的访问权限。

研究者们针对社交网络提供者制定访问控制策略而数据拥有者无法直接控制数据的问题, 使用基于属性加密机制, 提出各种各样的数据控制权转移的方案。例如, 文献[19]使用基于属性的加密算法、传统的公钥密码体制、自动密钥管理机制提出一个 **Persona** 模型, 实现了用户自己管理自己的信息。随着用户的不断加入和退出, 该方法已无法满足这种用户动态删除的情况。为了解决此问题, 文献[20]使用基于属性加密方案、代理机制, 提出一种高效的撤销机制, 提出 **EASiER** 模型, 实现在撤销单个用户的权限时不必对数据重新加密也不需要产生新的密钥, 从而满足了访问控制动态性要求。

表 2 从多个角度对目前基于属性的访问控制进行比较。可以看出, 基于属性加密的方式虽然能满足安全需求, 同时也能描述比较复杂的访问控制策略, 但通常这种方式需要比较大的计算开销, 同时也很难满足细粒度的访问控制模型, 因此, 在保证安全性和细粒度的前提下保证效率也

是研究的热点。

表 2

基于属性的访问控制模型

文献	分布式管理	细粒度	基于密码学	动态性	安全性
文献[19]	是	否	是	弱	强
文献[20]	是	否	是	强	强
文献[15]	否	否	否	弱	强
文献[16]	是	是	否	强	弱
文献[17]	是	是	否	强	弱
文献[18]	是	否	否	强	弱
文献[5]	是	是	否	强	弱

3.3 基于语义的访问控制模型

数据资源的语义信息显示了资源之间的内在联系, 从而提供了极为丰富的控制信息。依靠这些控制信息, 可对用户、资源、访问者进行限制从而构建细粒度的访问控制模型。语义网是一种描述语义信息的重要方式, 可以看作是在万维网数据资源的基础上添加语义元数据构建而成, 这些元数据蕴含了资源之间的内在联系。本体描述语言 (OWL, Web ontology language)^[21]能够描述资源之间的联系, 分离信息结构和内容, 形式化地描述信息, 是构建语义网的关键。使用本体描述语言不仅能够精确描述社交网络中用户、资源以及用户—资源之间的内在联系, 而且能对三者之间的关系进行形式化分析, 因而可以精确描述三者之间的限制条件。

研究者使用本体描述语言对社交网络中的用户、资源、策略以及各种限制条件等要素进行模拟, 并将访问控制中的相应操作映射对本体的操作。这种转化能够充分利用本体描述语言的形式

化分析能力。例如,针对 OSN 中访问控制模型的灵活性和可扩展性较差的问题,文献[22]通过语义网实体语言模拟社交网络各种概念,将访问控制策略和权限使用本体描述语言表示,将访问控制策略的执行转化为实体查询,从而增强访问控制的灵活性和可扩展性。文献[23, 24]对用户、资源以及用户—资源之间的复杂语义进行分析,通过使用资源描述框架(RDF, resource description framework)^[25]和 OWL 模拟策略,提出基于实体的访问控制模型。

社交网络中的访问控制模型不仅要考虑用户的社交关系因素,而且要考虑资源之间的语义因素。资源的语义不仅反映了资源之间的内在联系,而且体现出资源之间的逻辑关系,因此能够为访问控制策略提供限制条件。针对 OSN 中的访问控制策略仅考虑语法匹配而没有考虑语义信息的问题,文献[26]提出一种基于语义信息的访问控制模型。文献[27]通过事先定义的敏感词汇的语义信息自动识别新上传文件的敏感度,但此模型只能处理与预先定义词汇相关的限制信息。针对上述缺点,文献[28]使用语义网技术,通过使用知识库和语言工具代替上述事先定义的敏感词汇集,提出一种自动识别消息敏感等级的方法。在此基础上,提出了一种动态、透明、隐私驱动的访问控制模型。

3.4 其他的访问控制模型

研究者们针对社交网络、资源的不同特点,从多个角度提出了相应的访问控制模型。包括基

于上下文、基于可达性的访问控制模型等。

1) 基于上下文的访问控制模型

上下文的含义非常广泛,包括用户所处的环境和自身的状态,如时间、地点、位置等。基于上下文的访问控制模型(content-based access control)^[29]利用访问者的身份信息和所处的环境信息确定访问控制权限。文献[26]将用户数据同过去的某个事件进行关联,利用事件间的相似性,从过去的事件中寻找相似事件的知识并结合当前事件所涉及的上下文信息(如位置、时间、活动、参加者、倾向)实现访问权限的判定。该模型采用动态的策略判定方法,并且能够监督第三方服务器是否修改用户的数据。

2) 基于可达性的访问控制模型

可达性是指 2 个节点之间满足某些限制条件的性质。针对 Facebook 等社交网络中每个用户可根据某些特性对朋友进行分类并为每个类别定义相应访问控制策略的特点,文献[30]提出一种基于可达性的访问控制(context-based access control)模型。该模型依据节点间类型、方向、距离、可信级等限制条件的不同对访问控制权限进行判定。

3.5 模型的总结

研究者们针对社交网络的特点提出针对不同资源、不同需求的访问控制模型。如图 2 所示,社交网络中的访问控制研究可分为基于关系、基于属性、基于语义等访问控制模型。基于关系的访问控制模型通过引入关系类型、深度、直接关

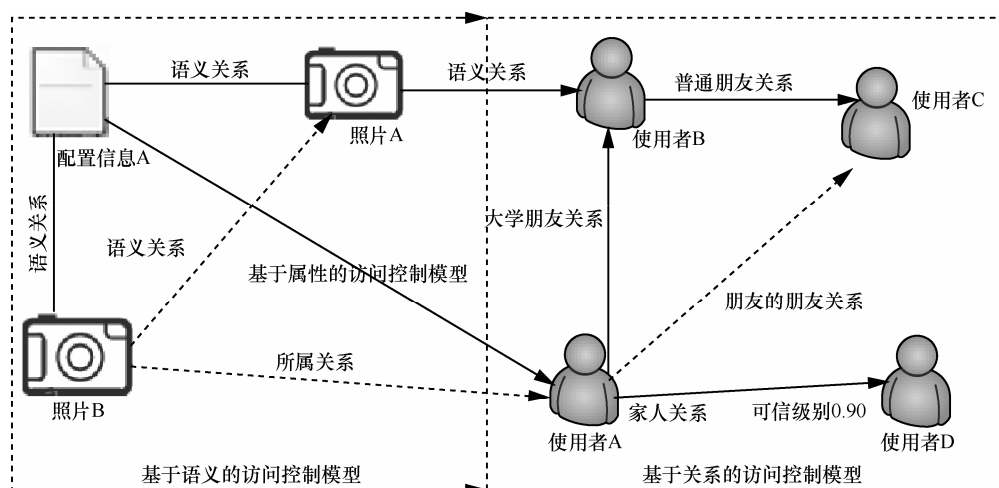


图 2 社交网络中的访问控制模型

系、间接关系、可信级别、属性因素、语义因素等,解决了访问者精细识别的困难问题。基于属性的访问控制模型利用访问控制中实体的固有属性,有效解决了社交网络中实体动态性强、数量较大所带来的问题。基于语义的访问控制模型在已有模型的基础上进一步考虑资源—资源、资源—用户、用户—用户间的语义关系及相应的语义信息逻辑关系等,使访问控制模型可以更准确地反映出用户的真实意图,保障资源的安全访问。

4 面向 OSN 的访问控制策略

4.1 策略的生成

社交网络中数据具有海量性、动态性等特点,手动标注策略不仅费时费力,而且容易产生错误,因此需要对策略自动生成方法进行研究。

研究者们使用某一标准将朋友划为不同的朋友群,并假设同一朋友群的用户具有相同隐私策略,进而提出不同的策略自动生成方案。例如,文献[31]采用聚类分析法分析,依据朋友列表的不同属性构建不同的社交圈子,根据社交圈子的属性生成对应的访问控制策略。文献[32]提出一个由辅助朋友群划分、相似朋友设定相似策略 2 个模型构成的策略管理模型。辅助朋友群划分模型采用聚类分析的方法划分朋友群,相似朋友设定相似策略模型根据朋友的用户历史信息和隐私倾向为此群设定同一策略。

研究者们依据社交网络结构、资源内容和标记、用户隐私倾向等提出不同的策略自动生成方案。例如,文献[33]利用用户位置预测其隐私倾向;文献[34]使用可信朋友的隐私策略为用户推荐策略,用户可根据自己的需求修改这些策略(该方案是从用户隐私倾向的角度修改隐私策略);文献[35]从资源的内容和元数据的角度针对社交网络中照片分享问题提出一个策略生成方案,该方案以图片内容和元数据为标准对图片进行分类,利用关联原则在同类照片集中进行策略挖掘,但此方案没有考虑社交网络结构因素。针对文献[34, 35]所提的 2 个方案都考虑因素不足的情况,文献[36]考虑社交网络结构、资源内容和元数据、用户隐私倾向等因素针对社交网络中照片分享问题,提出一个更精细的策略生成方案。

该方案在文献[35]方案的基础上额外解决了用户突然改变隐私倾向以及数据稀疏性问题。其处理过程为:用户通过模拟其朋友的隐私倾向,找出与自己具有相似隐私倾向的朋友,根据此朋友的数据挖掘相应的隐私策略。文献[37]采用配置文件属性、社交网络度量这 2 个给出用户相似性的度量方法,并以此作为策略授权依据,进而提出了策略推荐机制。

除此之外,研究者们使用机器学习自动识别文本信息的敏感度,并以敏感度作为控制要素制定相应的访问控制策略。例如,文献[27]使用预定义的敏感词作为训练集来识别新上传文本的敏感度,但该方案只能识别出训练集中的词汇。针对该问题,文献[28]使用知识库和语言工具自动识别上传文件的敏感度,解决了训练集数据不足的问题。

社交网络中的策略自动生成方案几乎都面临着冷开始和数据稀疏性问题,这极大限制了方案的精确性,因此,解决冷开始和数据稀疏性问题是重要研究方向。

4.2 策略的冲突消解

OSN 环境中数据具有强隐私性,每个数据相关者都想控制此数据。如用户 A 分享了一张敏感照片,该照片中牵涉 4 个用户,每个用户都想控制这张照片的权限以免泄露自己的隐私信息,但每个相关者对该照片的控制策略不同,可能会产生冲突,从而带来隐私泄露的风险。因此,如何准确识别和消解冲突策略是 OSN 中访问控制策略的重要研究点。

借鉴博弈论^[38,39],研究者们针对多方访问控制策略的冲突问题,提出不同的策略冲突消解方案。如文献[40]首次提出对社交网络中多方信息合作管理方案,该方案使用 Clarke-Tax^[41]机制将相关者的合作管理策略映射成拍卖方案,利用博弈论分析该拍卖方案,给出策略消解算法。在模型层面,文献[42, 43]解决了多方合作情况下访问控制模型和协议的设计问题。其中,文献[43]将利益相关方虚拟空间中的信息划分为配置信息、朋友关系、评论信息以及信息内容,并针对不同信息的特点制定相应的控制策略,最终采用投票的方式融合各方的控制策略,但在该方案中没有

考虑相关方的利益最大化的问题。针对该问题, 文献[44]使用博弈论分析利益相关者的策略, 将策略消解问题转化为多方博弈问题, 博弈问题的解就是相关者利益最大解, 但上述方案没有考虑相关者间可交互式的问题。针对此问题, 文献[45]通过假设相关者间不存在竞争、可以相互协商, 提出一个可调节各自控制策略的方案。文献[46]提出一种与非监督机制互补的交互式的策略调节机制。

上述控制策略的粒度都是文件级, 即控制某个(些)文件是否能被他人访问。文献[47]提出一个更细粒度的策略冲突消解方案。该方案使用人脸识别技术^[48]识别出照片中每个人脸对应的关系者, 关系者确定控制策略, 从而解决了关系者间的策略冲突问题。

4.3 策略的验证

策略验证的基本思路是使用模型抽象策略, 并对策略和要验证的性质进行形式化描述, 根据形式化描述验证策略与性质之间的对应关系^[49-51]。

文献[43, 52, 53]使用回答集编程(ASP, answer set programming)^[54,55]模拟策略, 利用 ASP 解法器进行自动分析, 从而将策略的相关问题转化对 ASP 的查询问题。其中, 文献[43]针对于策略授权问题, 文献[52,53]针对于策略安全性问题。

5 结束语

社交网络的快速发展使用户的隐私问题日益严峻, 访问控制作为信息保护的关键技术势必成为社交网络中数据保护的重要手段。本文首先概述了社交网络的基本特点; 然后从这些特点出发阐述了基于关系、基于属性、基于语义等访问控制模型, 分析了这些模型的发展历程、优缺点、适应的场景, 并讨论了这些模型未来的发展趋势; 最后, 分析了自动策略生成的各种方案、各种假设条件下的冲突消解方案、策略验证方案。

参考文献:

- [1] NI M, ZHANG Y, HAN W, et al. An empirical study on user access control in online social networks[C]//The 21st ACM Symposium on Access Control Models and Technologies, Shanghai. c2016: 13-23.
- [2] HART M, JOHNSON R, STENT A. More content-less control: access control in the Web 2.0[J]. IEEE Web, 2007, 2.

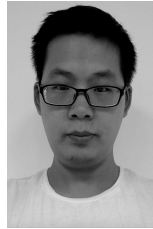
- [3] ALI B, VILLEGAS W, MAHESWARAN M. A trust based approach for protecting user data in social networks[C]//The 2007 Conference on Collaborative Research, Richmond Hill. c2007: 288-293.
- [4] FONG P W L, ANWAR M, ZHAO Z. A privacy preservation model for facebook-style social network systems[C]// European Symposium on Research in Computer Security, Heidelberg. c2009: 303-320.
- [5] NIN J, TORRA V. Possibilistic reasoning for trust-based access control enforcement in social networks[C]//IEEE International Conference on Fuzzy Systems, Barcelona. c2010: 1-6.
- [6] VILLEGAS W, ALI B, MAHESWARAN M. An access control scheme for protecting personal data[C]//The 6th Conference on Privacy, Security and Trust. c2008: 24-35.
- [7] CARMINATI B, FERRARI E, PEREGO A. Enforcing access control in Web-based social networks[J]. ACM Transactions on Information and System Security (TISSEC), 2009, 13(1): 6.
- [8] CHENG Y, PARK J, SANDHU R. Relationship-based access control for online social networks: beyond user-to-user relationships[C]// International Conference on Privacy, Security, Risk and Trust. c2012: 646-655.
- [9] FONG P W L. Relationship-based access control: protection model and policy language[C]// ACM Conference on Data and Application Security & Privacy. c2011: 191-202.
- [10] FONG P W L, SIAHAAN I. Relationship-based access control policies and their policy languages[C]//The 16th ACM Symposium on Access Control Models and Technologies. c2011: 51-60.
- [11] RIZVI S Z R, FONG P W L, CRAMPTON J, et al. Relationship-based access control for an open-source medical records system[C]//ACM Symposium on Access Control Models and Technologies. c2015: 113-124.
- [12] 李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型[J]. 通信学报, 2008, 29(4): 90-98.
- LI X F, FENG D G, CHEN Z W, et al. Model for attribute based access control[J]. Journal on Communications, 2008, 29(4): 90-98.
- [13] 沈海波, 洪帆. 面向 Web 服务的基于属性的访问控制研究[J]. 计算机科学, 2006, 33(4): 92-96.
- SHEN H B. Study on attribute-based access control for Web services[J]. Computer Science, 2006, 33(4): 92-96.
- [14] 王小明, 付红, 张立臣. 基于属性的访问控制研究进展[J]. 电子学报, 2010, 38(7): 1660-1667.
- WANG X M, FU H, ZHANG L C. Research progress on attribute-based access control[J]. Acta Electronica Sinica, 2010, 38(7): 1660-1667.
- [15] HSU A C, RAY I. Specification and enforcement of location-aware attribute-based access control for online social networks[C]//ACM International Workshop on Attribute Based Access Control. c2016: 25-34.
- [16] CHENG Y, PARK J, SANDHU R. Attribute-aware relationship-based access control for online social networks[C]//IFIP Annual Conference on Data and Applications Security and Privacy. c2014: 292-306.

- [17] CHENG Y, PARK J, SANDHU R. Attribute-aware relationship-based access control for online social networks[C]//IFIP Annual Conference on Data and Applications Security and Privacy, Vienna. c2014: 292-306.
- [18] PANG J, ZHANG Y. A new access control scheme for facebook-style social networks[C]//International Conference on Availability, Reliability and Security. c2013:1-10.
- [19] BADEN R, BENDER A, SPRING N, et al. Persona: an online social network with user-defined privacy[J]. ACM Sigcomm Computer Communication Review, 2009, 39(4):135-146.
- [20] JAHID S, MITTAL P, BORISOV N. EASIER: encryption-based access control in social networks with efficient revocation[C]//ACM Symposium on Information, Computer and Communications Security. c2011:411-415.
- [21] 史斌. 面向语义网的语义搜索引擎关键技术研究[D].北京: 北京工业大学, 2010.
- BIN S. The research on key technology of semantic search engine in semantic Web[D]. Beijing: Beijing University of Technology, 2010.
- [22] CARMINATI B, FERRARI E, HEATHERLY R, et al. Semantic Web-based social network access control[J]. Computers and Security, 2011, 30(2).
- [23] HORROCKS I, PATEL-SCHNEIDER P F, BOLEY H, et al. SWRL: a semantic Web rule language combining OWL and rule ML[J]. W3C Member Submission, 2004, 21: 79.
- [24] CARMINATI B, FERRARI E, HEATHERLY R, et al. A semantic Web based framework for social network access control[C]//ACM Symposium on Access Control Models and Technologies. c2009:177-186.
- [25] 文峰. 一种面向应用的多层次数据资源描述框架[J]. 计算机应用与软件, 2013, 30(7):221-223.
- WENG F. An application-oriented multi-level data resource description frame[J]. Computer Applications & Software, 2013, 30(7):221-220.
- [26] JADLIWALA M, MAITI A, NAMBOODIRI V. Social puzzles: context-based access control in online social networks[C]//Annual IEEE/IFIP International Conference on Dependable Systems and Networks. c2014: 299-310.
- [27] VILLATA S, COSTABELLO L, DELAFORGE N, et al. A social semantic Web access control model[J]. Journal on Data Semantics, 2012, 2(1):21-36.
- [28] IMRAN-DAUD M, SÁNCHEZ D, VIEJO A. Privacy-driven access control in social networks by means of automatic semantic annotation[J]. Computer Communications, 2016, 76:12-25.
- [29] 徐仁佐, 郑红军, 陈斌, 等. 基于角色和上下文的访问控制模型[J]. 计算机应用研究, 2004, 21(12):140-142.
- XU R Z, ZHENG H J, CHEN B, et al. Role and context-based access control model[J]. Application Research of Computers, 2004.
- [30] ABDESSALEM T, DHIA I B. A reachability-based access control model for online social networks[C]//ACM Symposium on Databases and Social Networks. c2011: 31-36.
- [31] KAPADIA A, ADU-OPPONG F, GARDINER C K, et al. Social circles: tackling privacy in social networks[C]//Symposium on Usable Privacy Security. 2008.
- [32] CHEEK G P, SHEHAB M. Policy-by-example for online social networks[C]//ACM Symposium on Access Control Models and Technologies. c2012:23-32.
- [33] RAVICHANDRAN R, BENISCH M, KELLEY P, et al. Capturing social networking privacy preferences[C]//Symposium on Usable Privacy Security, California. c2009: 1-18.
- [34] BONNEAU J, ANDERSON J, CHURCH L. Privacy suites: shared privacy for social networks[C]//Symposium on Usable Privacy and Security, California. c2009.
- [35] SQUICCIARINI A C, SUNDARESWARAN S, LIN D, et al. A3P: adaptive policy prediction for shared images over popular content sharing sites[C]//ACM Conference on Hypertext and Hypermedia, Eindhoven. c2011:261-270.
- [36] SQUICCIARINI A C, LIN D, SUNDARESWARAN S, et al. Privacy policy inference of user-uploaded images on content sharing sites[J]. IEEE Transactions on Knowledge & Data Engineering, 2015, 27(1):193-206.
- [37] SHEHAB M, TOUATI H. Semi-supervised policy recommendation for online social networks[C]//International Conference on Advances in Social Networks Analysis and Mining. c2012:360-367.
- [38] 张慧, 方旭明. 基于价格理论和博弈论的接入控制策略[J]. 通信学报, 2008, 29(7):94-102.
- ZHANG H, FANG X M. Pricing and game theory based admission control scheme[J]. Journal on Communications, 2008, 29(7): 94-102.
- [39] 田有亮, 马建峰, 彭长根, 等. 秘密共享体制的博弈论分析[J]. 电子学报, 2011, 39(12):2790-2795.
- TIAN Y L, MA J F, PENG C G, et al. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12):2790-2795.
- [40] SQUICCIARINI A C, SHEHAB M, PACI F. Collective privacy management in social networks[C]//International Conference on World Wide Web. c2009:521-530.
- [41] EPHRATI E, ROSENSCHEIN J S. The clarke tax as a consensus mechanism among automated agents[C]//National Conference on Artificial Intelligence. c1991, 91: 173-178.
- [42] SQUICCIARINI A C, XU H, ZHANG X. CoPE: enabling collaborative privacy management in online social networks[J]. Journal of the American Society for Information Science & Technology, 2011, 62(3):521-534.
- [43] HU H, AHN G J, JORGENSEN J. Multiparty access control for online social networks: model and mechanisms[J]. IEEE Transactions on Knowledge & Data Engineering, 2013, 25(7):1614-1627.
- [44] HU H, AHN G J, ZHAO Z, et al. Game theoretic analysis of multiparty access control in online social networks[C]//ACM Symposium on Access Control Models and Technologies. c2014:93-102.
- [45] XIAO Q, TAN K L. Peer-aware collaborative access control in social networks[C]//International Conference on Collaborative Computing:

Networking, Applications and Worksharing. c2012:30-39.

- [46] MEHREGAN P, FONG P W L. Policy negotiation for co-owned resources in relationship-based access control[C]//ACM on Symposium on Access Control Models and Technologies. c2016: 125-136.
- [47] ILIA P, POLAKIS I, ATHANASOPOULOS E, et al. Face/off: preventing privacy leakage from photos in social networks[C]//The 22nd ACM Sigsac Conference on Computer and Communications Security. c2015: 781-792.
- [48] ZHANG C, ZHANG Z. A survey of recent advances in face detection[EB/OL]. http://research.microsoft.com/en-us/um/people/chazhang/publications/tr2010-66_Chazhang.pdf.
- [49] 包义保, 殷丽华, 方滨兴, 等. 基于良基语义的安全策略表达与验证方法[J]. 软件学报, 2012, 23(4): 912-927.
BAO Y B, YIN L H, FANG B X, et al. Approach of security policy expression and verification based on well-founded semantic[J]. Journal of Software, 2012, 23(4):912-927.
- [50] 包义保, 殷丽华, 方滨兴, 等. 动态安全策略逻辑语言及安全属性验证问题的研究[J]. 计算机研究与发展, 2010, 50(5): 932-941.
BAO Y B, YIN L H, FANG B X, et al. Logic-based dynamical security policy language and verification[J]. Journal of Computer Research & Development, 2013, 50(5):932-941.
- [51] BONATTI P, SHAHMEHRI N, DUMA C, et al. Rule-based policy specification: state of the art and future work[EB/OL]. <http://www.macs.hw.ac.uk/bisel/reverse/deliverables/i2-d1.pdf>.
- [52] JAKOB M, MOLER Z, PECHOUCEK M, et al. Intelligent content-based privacy assistant for facebook[C]//The IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology. c2011: 499-500.
- [53] RATHORE N C, TRIPATHY S. Collaborative access control model for online social networks[C]//ICDCIT. c2016.
- [54] LIFSCHITZ V. Answer set programming and plan generation[J]. Artificial Intelligence, 2002, 138(1): 39-54.
- [55] LIFSCHITZ V. Answer set planning[C]//International Conference on Logic Programming and Nonmonotonic Reasoning. c1999: 373-374.

作者简介:



陈天柱 (1987-), 男, 河北秦皇岛人, 中国科学院信息工程研究所博士生, 主要研究方向为信息安全。



郭云川 (1977-), 男, 四川营山人, 博士, 中国科学院信息工程研究所副研究员, 主要研究方向为物联网安全、形式化方法。



牛犇 (1984-), 男, 陕西西安人, 博士, 中国科学院信息工程研究所助理研究员, 主要研究方向为网络安全、信息保护。



李风华 (1966-), 男, 湖北浠水人, 博士, 中国科学院信息工程研究所副总工、研究员、博士生导师, 主要研究方向为网络与系统安全、信息保护、隐私计算。