第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0565-11

社交网络安全问题及其解决方案

刘建伟,李为宇,孙 钰

(北京航空航天大学电子信息工程学院,北京 100191)

摘要:社交网络(social network,SN)具有用户数目多、数据量大、信息开放、用户关系难以管理等特点.如何实现用户隐私保护、身份认证和数据访问控制,已成为社交网络中备受关注的安全问题.本文首先介绍了社交网络的基本概念、发展现状和主要技术,并结合社交网络的特点,从社交网络数据挖掘、传统威胁、身份窃取等方面分析其存在的主要安全威胁,总结其存在的安全风险.然后,阐述了几种较为完善的社交网络安全解决方案,并对其工作原理进行了分析和比较.最后,给出了社交网络安全研究的几个热点研究课题,并讨论了社交网络安全性研究的发展方向.

关键词:社交网络安全;隐私保护;身份认证;访问控制

中图分类号:TP393.02 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.001

Security issues and solutions on social networks

LIU Jianwei, LI Weiyu, SUN Yu

(*School of Electronics and Information Engineering, BeiHang University, Beijing* 100191, *China*)

Abstract: Social networks (SN) have the characteristics of immensity of data, huge clientele, openness in information sharing, difficult customer relationship management, etc. Security issues, such as privacy protection, identity authentication and data access control have increased enormously on such networks. The basic concept, present development and main technology of SN were introduced. And specific security risks according to its characteristics were also summarized from the aspects of data mining, traditional threats and identity theft on SN. Furthermore, several existing security solutions of SN were described, and their working principles were analyzed and compared. Finally, some hot security research topics were given and the future research directions were discussed.

Key words: social network security; privacy protection; identity authentication; access control

收稿日期:2011-05-04;**修回日期**:2011-07-13

基金项目:中国高技术研究发展(863)计划(2009AA01Z418),中央高校基本科研业务费专项资金(YWF1002009),中国博士后科学基金(20090460192)资助.

作者简介:刘建伟(通讯作者),男,1964年生,教授,博士生导师.1988年于山东大学获理学硕士;1998年于西安电子科技大学获工学博士;现任北京航空航天大学教授.先后从事移动通信网络、Ad hoc网络、无线传感器网络、无线mesh网络、社交网络、车辆自组织网络、云计算等的保密和认证技术研究.主持和参与国家863课题、国家自然科学基金项目、工信部电子发展基金项目、国家经贸委国家技术创新项目计划、国防基础科研项目等课题10余项,发表论文40余篇,出版专著和教材5部,其中专著《通信网的安全——理论与技术》获教育部优秀教材一等奖.主持开发的"FW3031AG防火墙"获山东省科学技术进步三等奖,"Netkey身份认证系统"获山东省计算机应用新成果二等奖.目前兼任教育部高等学校信息安全类专业教学指导委员会委员,工信部电子发展基金专家,高等学校信息安全专业系列教材编委,中国海洋大学兼职教授,计算机网络与信息安全教育部重点实验室(西安电子科技大学)客座研究员.

E-mail:liujianwei@buaa.edu.cn

0 引言

0.1 社交网络的概念及特点

社交网络[1](social network,SN)是源于社会网络关系系统思想的网络应用形式,旨在帮助人们建立社会性网络的互联网应用服务,由代表不同个人或团体的节点构成,呈现出实体之间的关系网络,为用户提供如下主要功能:

①在一定范围内,创建并分享公开或半公开的用户信息;

②提供可联系的用户列表,为用户提供交往平台;

③网络聊天、交友、视频分享、博客、网络社区、音乐共享、添加评论等;

④提供用于应用插件开发的开放接口.

社交网络在很大程度上为人们的社会交往提供了方便,也因此具备如下几个主要特点:

①用户数目多,用户群种类复杂且交互方式多样;

②应用灵活,功能繁多,用户行为难以控制;

③信息量大,开放程度高,数据存储集中,管理难度大.

这些特点的存在使得社交网络的安全问题尤为突出.为了利用这个交往平台,人们乐于将自己的个人信息,如爱好、日志、照片、状态,甚至姓名、生日等在社交网络上与他人共享,如果没有良好的保护手段,用户信息的私密性将受到严重威胁.近些年,私密信息泄露、用户信息非法出售、用户身份假冒等诸多问题不断出现.因此,安全高效的隐私保护和访问控制方案成为社交网络安全领域的重要研究内容.

0.2 社交网络安全现状

社交网络作为一种虚拟社交媒介,为用户提供了保持联系、分享信息的平台.对于社交网站的攻击一般指窃取和非法使用用户的非公开信息,这些私密信息可能被直接使用,也可能被非法出售.由于人们为了达到沟通交流的目的,都乐于将自己的信息发布在各种社交网站上;因此,如果没有隐私保护的意识和相应技术防范,那么社交网站的安全使用将无法得到保障.通过社交网络,攻击者可以获得用户信息以及不同用户之间的相互关系,并用于传播未经许可的和欺骗性的消息.例如,攻击者窃取用户的联系列表后,伪装成为该用户并向该联系列表中的其他用户发送虚假信息.所获得的用户信息还可以被用于各种网络钓鱼和鱼叉式网络钓鱼[2-4].

经过10年左右的发展,众多的社交网络已经被全世界各地的网络用户所接受,并逐步成为人们社会交往的必要工具.随着用户的不断增多,通过社交网站发布的个人信息也越来越多,因此,用户信息的隐私保密和应用安全问题也得到了越来越多的重视.

如下几个事件,反映了社交网络的安全隐患[5]:

①2005年,针对MySpace,发生了名为Sammy的蠕虫攻击.Sammy利用MySpace的漏洞,并能快速传播.虽然Sammy的目的不在于窃取用户信息,但是对MySpace的运营造成了严重的影响.

②2009年4月,针对Twitter,发生名为Mikeyy的蠕虫攻击.Mikeyy篡改了用户的页面内容,依然没有窃取用户信息.

③随后,2009年5月,针对Facebook,发生了名为Koobface的蠕虫攻击.这次不像前两次那么幸运,Koobface窃取了诸如用户密码等用户私密信息.此后,Koobface又在其他社交网络上传播,并且其危害越发严重.

本文结合社交网络的特点,从隐私泄露、传统威胁、身份窃取等方面分析其主要安全问题,总结安全社交网络方面的研究热点;同时,以此为基础阐述了几种较为完善的安全社交网络解决方案,分析其工作原理;并提出了安全社交网络研究领域的开放性问题和发展方向.

1 社交网络的发展

1.1 发展历史

最初,在一定程度上具有社交网络特点的网站出现于1997年.SixDegrees作为第一个全面的社交网络始于1998年,并于2000年关闭.SixDegrees为用户提供了互相联系和发送信息的平台,是社交网络发展的开端.1997年至2001年是社交网络发展的第一阶段,这期间,出现了许多具有社交网络功能的在线工具,用户可以创建个人信息并可以实时更新,并且,用户通过这些个人信息就可以区分出自己的好友.社交网络发展的下一个阶段自2001年开始,其标志是Ryze的创建,出现了应用于商业领域的社交网络平台.随后,自2003年起,大量的社交网络网站相继出现,种类也不断变化.

社交网络的快速发展呈现出全球趋势，除了著名的 MySpace，Facebook，Flickr 等，还有巴西的 Orkut，日本的 Mixi，瑞典的 Lunarstorm，波兰的 Grono 以及在英国、新西兰等地流行的 Bebo 等. 在中国，QQ 是最早以软件形式形成的社交网络，后来的开心网、人人网、51. com、豆丁网等都在不同用户群体之间得到了广泛的发展.

1.2　典型案例

典型的社交网络有如下几个[6-7]：

典型案例 1　MySpace

一个点对点（P2P，peer to peer）的基于媒体的社交网络，其中的成员可以创建并维护他们的个人网页. MySpace 在 2003 年起源于洛杉矶，最初，他是一个面向音乐的交流网站，设计的初衷是为乐队、音乐家和音乐爱好者搭建交流的平台. 因此，其核心概念在于媒体共享，现在，其功能已经远远超出最初形式.

MySpace 的不足在于，不仅注册用户之间，任何一个上网者都可以访问注册用户的个人主页，因此，没有足够的隐私保护措施. 但是其强调，用户音乐、视频等信息只能存储在注册用户空间内，这样其他用户只能访问，而不能获取，保证了原创用户的版权和信息保护.

典型案例 2　Facebook

在 2004 年 2 月，由一个哈佛大学的二年级学生创建，最初它只在哈佛大学中使用，两年之后，发展成为面向所有大学和中学的社交网络平台. Facebook 基于用户间关系创建用户资料，并反映出他们在日常生活中的紧密联系. Facebook 的超前之处在于，它已经成为一种平台化的服务形式，向第三方开发者提供了用于应用程序开发的开放接口，开发者在平台基础上开发自己的应用软件，并无缝嵌入 Facebook 中.

隐私保护同样是 Facebook 考虑的技术问题之一. 一方面，由于 Facebook 用于校园内部，通过学校管理和法律权威机构来认定用户的不合法行为，这种管理模式在一定程度上提高了用户规范自身行为的意识；另一方面，为用户提供了隐私设置功能，以便决定哪些信息可以被哪些用户和开发者获取.

典型案例 3　LinkedIn

创建于 2002 年 12 月，是一种商业性的社交网站，其目的是帮助注册用户维护他们在商业中信任人的详细联系列表. 每个列表中的一项纪录称为一个连接（connection），注册用户可以邀请或推荐其他人或事物作为“连接”中的一员，这些“连接”的作用是：

①用户可以通过其他人在联系列表中推荐的“连接”寻找工作、商机甚至是某个人；

②招聘者可以列出推荐职位列表来寻找到潜在的申请者；

③用户可以发布自己的照片、视频等作为身份的标识；

④求职者可以查看招聘者的推荐列表，并发现哪些现有的用户也可作为他们的推荐者.

典型案例 4　Wikipedia

是一种合作式的在线百科全书项目，任何人都可以在其上创建和编辑内容. Wikipedia 被基金组拥有，Wikipedia 基金组是一个非盈利型组织，用来开发和维护用户提供的开放数据. Wikipedia 的用户在后台完成网站内容的编辑，并讨论信息的可靠性和真实性. 编辑们可以查看文章的修改历史，如果发现了恶意篡改或虚假内容，则将其恢复到未被修改之前的状态. 任何人都可以修改网站内容，因此，Wikipedia 对恶意篡改行为非常敏感，其提供的信息是否可靠也一直被人们所讨论.

典型案例 5　YouTube

一个在线视频分享网站，允许用户上载视频、电影等，其他用户可以免费浏览并保存. YouTube 的管理通过社区形式，人们可以对自己看到的视频进行评论或标记，维护人员检查这些评论和标记，如果评论中包含恶意内容，或评论和标记中反映出视频内容不合法，则采取措施加以禁止.

2　社交网络安全问题分析

作为一种计算机网络的应用形式，社交网络中的各种安全问题与传统计算机网络安全问题有很多相似之处；但是，由于社交网络自身的开放性，又出现了许多针对其自身特点的攻击方式，主要可分为 3 个类别. 本部分内容将对社交网络中不同类别的安全问题进行分析和总结[5,8-11].

2.1　针对社交网络的数据挖掘

（Ⅰ）数字档案收集

社交网络中的用户信息可被第三方组织下载、收集，随着不断积累，最后可以形成关于这个用户的完整档案，并用于非法用途.

(Ⅱ) 运维数据收集

除了用户的公开可见信息,还有一些网络运维数据,如上线时长、接入位置(IP)、消息发送和接收、一个用户对其他用户信息的浏览等.这些数据可被用于目标定位、识别或者向第三方转发数据等.

(Ⅲ) 人脸识别

很多社交网站将照片作为用户信息的一部分,有些网站还显性或隐性地将照片作为身份标识.如果攻击者成功应用人脸识别[12],就可以交叉访问同一用户在不同网站上的个人信息.

(Ⅳ) 图像数据标记

大多数社交网站为用户提供了在照片上圈出某块区域在其上做标记[13]的功能,但没有提出相应的保护方案,这样会出现隐私信息被窃取的情况,例如:在照片中圈出某个人,标记其邮箱、电话、地址、姓名等信息.这不仅会威胁到社交网络用户的隐私,而且对照片上出现的任何人都会造成影响.

2.2 传统形式的安全威胁

(Ⅰ) 垃圾信息传播

传统的垃圾信息攻击是通过电子邮件大量传播垃圾邮件,对于社交网络,各种垃圾信息,包括广告和恶意代码等,可以通过好友列表快速传播.其危害主要有:

①增加网络负载.

②信任缺失.通过好友申请或其他引诱手段,达到钓鱼、链接重定向等目的.

③身份假冒.攻击者创建大量虚假用户并伪造用户信息,当数量过多时,将会超出网络自身的适应能力.

(Ⅱ) 破坏系统可用性

攻击者可以通过各种手段增加网络负载、将用户请求重定向或破坏网络数据的可用性等,最终达到影响网络性能、破坏系统服务的目的.常见的攻击方式主要有拒绝服务攻击、黑洞攻击、错误路由等.

(Ⅲ) 第三方软件及插件

由于众多的社交网络都为第三方开发者提供免费的应用程序开放接口,任何人都可以根据自己的兴趣爱好开发并向网站中嵌入自由开发的应用程序,同时,各种 Flash,Silverlight 等运行于浏览器上的插件都可被攻击者利用.其主要危害有:

①引入更多的软件漏洞和插件漏洞;

②使得一些只用简单用户名/密码作为认证方式的网站更为脆弱,增加了身份窃取威胁;

③为用户信息搜集提供了机会,攻击者可以利用开放接口开发专门用于信息收集的软件,并嵌入社交网站,达到窃取重要信息的目的;

④增加基础信息数量,使得用户的隐私保密更难控制;

⑤带来 XSS 攻击,攻击者向 Web 页面里插入恶意代码,在用户浏览该页时,达到窃取账户信息、迫使用户下载恶意软件、触发恶意链接等目的.

(Ⅳ) 污染攻击(pollution attack)[14]

这种攻击方式主要带来两方面的危害:一方面,攻击者对目标数据加入噪声或进行篡改以达到传播虚假信息、破坏数据可用性的目的;另一方面,攻击者伪造服务器 IP 地址,将用户访问引导至不提供服务的 IP 地址,破坏系统可用性.

(Ⅴ) 用户名及密码窃取

这是最传统的攻击形式,威胁到用户的登录认证安全.如果用户名和对应的密码被窃取,那么,攻击者就可以顺利登录系统,获取注册用户使用系统的特殊权限,或以被盗用户的名义进行非法操作.

2.3 与身份相关的威胁

(Ⅰ) 通过社交网络的网络钓鱼(phishing)和渔叉式网络钓鱼(spare phishing)[15]

在社交网络中,攻击者可以伪装成为合法用户的好友,通过各种诱惑手段使得用户访问恶意 URL.由于社交网络用户为了达到结交朋友的目的,并不排斥与陌生人沟通并接受交友邀请,因此,钓鱼攻击就很容易发生.

(Ⅱ) Sybil 攻击[16]

攻击节点在实施 Sybil 攻击时,会伪装成为多种身份参与到正常网络中,一方面利用虚假身份盗取合法用户的各种数据,另一方面影响数据转发路径,从而可伪造出多条不同的、甚至是互不相交的路由,破坏网络的可用性.

(Ⅲ) Wormhole 攻击[17]

这种攻击方式主要针对移动社交网络,攻击者在网络的一端接收报文,通过特殊的快捷通道将报文传送到网络的另一端后再重播.例如,合法用户在网络一端向服务器发送身份标识及数据请求报文,攻击者在其附近截获此报文并在网络的其他地方重放此段报文,一方面假冒原有用户窃取信息,另一方面对获取的数据实施各种选择丢弃、篡改、重播等,

也有可能发生泛洪攻击.

3　安全社交网络典型解决方案

针对前文所述的不同种类的安全问题,不同类型的安全社交网络解决方案不断出现.本节内容阐述 5 种典型的安全社交网络解决方案的基本原理,并加以分析.

3.1　VisualSec

在社交网络中,一些用户之间的交互信息带有一定的私密性,不能被其他人随意读取,因此,设计相应的安全消息转发方案是必要的.安全的消息转发应该满足如下两个基本要求:

①认证性:方案应该能够保证,消息接收方就是消息发送方指定的目的用户.假冒攻击等应当被有效避免.

②保密性:方案应该保证所有用户都经过身份认证,未经认证的用户不可获取敏感信息.合理的访问控制机制应当避免攻击者的非法接入.

文献[18]以 ID-based[19]为基础,根据社交网络应用场景,提出了 VisualSec 方案. ID-based 是 Shamir 在 1984 年为了简化 PKI 中证书和密钥管理而设计的.在 ID-based 方案中,密钥生成中心(KGC,key generate center)验证用户身份的合法性,然后通过用户身份标识符为用户生成私钥,并直接将用户身份标识符作为用户公钥.

在 ID-based 和传统 PKI 加密方案中,唯一用户名或电子邮件地址等都可作为用户身份标识符.但是,一方面,目前众多社交网络均由各服务提供方独立运营,密钥生成中心由服务提供方建立,而不是可信第三方,在这种情况下,社交网络系统的管理员就是一个潜在的攻击者,如果直接采用 ID-based 方案,无法保证密钥生成过程的可靠性;另一方面,社交网络用户多数使用昵称或假名,无法保证其唯一性和真实性,而且,在社交网络中,电子邮件地址等信息本身就是一种隐私信息,将其作为用户身份标识符是不安全的.

VisualSec[18]方案考虑到在大多数社交网络中,头像照片是一种公开信息,容易获取并且可以直观地反映用户身份,利用这样的照片作为用户身份标识符是一种可行方案.

3.2　Social-K

随着智能手机、掌上电脑等便携设备的不断完善,移动社交网络也逐渐出现在人们的生活当中.所谓移动社交网络是指,在移动设备上安装第三方软件,用户通过这样的应用软件在第三方服务器进行注册和认证,第三方服务器在原有社交网络中获取该用户在社交网络中的身份标识,并将其与移动用户身份绑定,根据移动用户发出的操作请求在社交网络中获取相应数据并转发给移动用户.现有的移动社交网络系统有 WhozThat, CenceMe, Loopt, Serendipity 等.移动社交网络也存在很多安全问题,最主要有两个方面:

①第三方服务器直接使用原有社交网络中的身份标识进行身份认证,并获取数据,由于无线数据链路的开放性,用户在社交网络中的身份标识很容易被窃取.

②用户信息私密性无法得到保护.如果攻击者截获了一部分用户信息,就有可能映射出这些信息所对应的一个或几个用户.

文献[20-22]提出了解决上述第一个问题的解决方案,系统结构如图 1 所示.

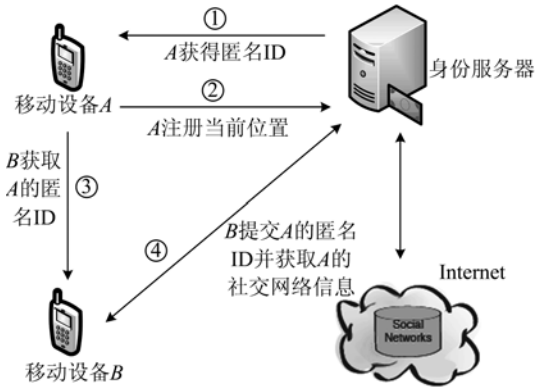

图 1　Social-K 访问控制流程图

Fig. 1　Access control flow diagram of Social-K

移动设备 A 和 B 通过蓝牙等方式参与通信,都可以与身份服务器进行交互,一个用户想要获取其他用户的社交网络数据时,要经过图中所示的如下步骤:

①B 向 A 发出访问请求,A 通过身份服务器获得随机生成的匿名 ID,同时,身份服务器将 A 的匿名 ID 与 A 的社交网络 ID 进行关联,使两者一一对应.

②A 向身份服务器注册自己当前的位置信息,这样,如果有攻击者在网络的其他位置重放报文,身份服务器就可以发现,进而防止虫洞攻击.

③A 向 B 发送自己的匿名 ID.

④B 向身份服务器发送 A 的匿名 ID 及查询请求，身份服务器根据步骤①中的关联关系，通过 A 的匿名 ID 获取其社交网络 ID，进而获取 A 的社交网络数据并转发给 B. 查询成功后，此次为 A 分配的匿名 ID 则失效.

在此方案中，移动网络侧全部使用匿名 ID，且每个匿名 ID 使用一次则失效，保证即使被攻击者截获，也无法对社交网络系统实施攻击. 同时，移动终端要向身份服务器注册位置信息，如果消息发送方超出距离范围则拒绝提供服务，可有效防止虫洞攻击.

文献[20]提出了解决上述第二个问题的解决方案，其系统结构如图 2 所示.

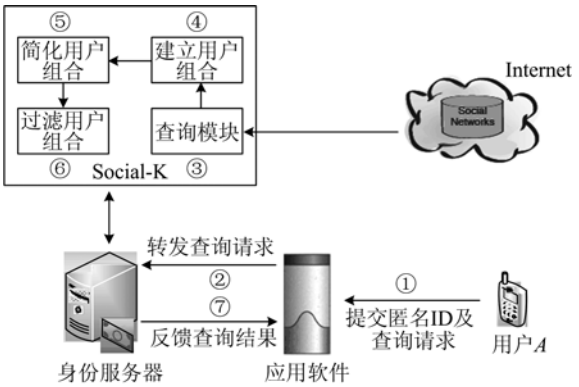

图 2 采用 K-Anonymity 模型的 Social-K 系统结构示意图

Fig. 2 System architecture of Social-K based on K-Anonymity

该系统在图 1 基础上添加了 Social-K 部分，这一部分是以 K-Anonymity 模型[23]理论为基础设计的用户隐私保护方案.

下面，通过一个简单的例子说明 K-Anonymity 的原理. 如表 1 所示，假设其是一组社交网络上发布的个人信息，如果有攻击者获得了这样一个信息组合：<Red，A，1>，那么就可以判断出这组数据对应 5 组用户组合：<Bill>，<Fred，Joe>，<Bill，Joe>，<Bill，Fred>，<Bill，Fred，Joe>. 通过逻辑简化算法得到这 5 个组合中的两个最小组合为：<Bill>和<Fred，Joe>，即信息组合<Red，A，1>对应组合<Bill>或<Fred，Joe>. 如果我们定义最小用户组合的数目为隐私强度系数 k，那么在这个例子中 k 就为 2. k 值越大，隐私强度越高，通过一组公开信息映射出对应用户的难度也就越大. 隐私强度系数的选取要根据系统的安全需求而定.

表 1 K-Anonymity 原理示例

Tab. 1 An example for the principle of K-Anonymity

Name	Color	Letter	Number
Bill	Red	A	1
Fred	Green	A	2
Jon	Green	B	1
Joe	Red	C	1

Social-K 方案的工作步骤按图 2 所示如下：

（Ⅰ）用户 A 通过移动设备上的应用软件向身份服务器提出对于自身公开信息组合的查询请求.

（Ⅱ）身份服务器将查询请求转发给 Social-K，然后 Social-K 通过图中模块③查询所有与用户 A 公开信息组合相关的其他用户信息.

（Ⅲ）Social-K 通过模块④建立所有对应用户组合.

（Ⅳ）Social-K 通过模块⑤找到最小用户组合.

（Ⅴ）Social-K 通过模块⑥对步骤（Ⅰ）提交的信息组合进行过滤. 即如果步骤（Ⅳ）中得到的最小用户组合的数目小于预先设定的隐私强度系数，那么，公开发布这样的信息组合是不安全的，应当将其中的一部分去掉，重新进行查询过程，直到最小用户组合数目大于或等于隐私强度系数为止.

3.3 Safebook

目前，多数运营商将用户信息永久保存在中心服务器，容易引起信息大规模泄漏. Safebook[24-26]针对此问题基于 P2P 形成无中心社交网络架构，防止了在中心服务器控制的情况下用户数据大规模泄漏的情况. 其提供了有效的信任关系管理，提高合法节点间的合作特性. 每个节点代表一个参与实体，由假名或者节点标识符唯一标识，并在逻辑上将好友作为邻居节点，采用 DHT 算法-Kademlia[27]设计了基于邻居节点代理的信息存储、转发和查找方案，保证匿名特性和查找效率. 并采用 PKI 作为基本的保密措施. 图 3 展示了 Safebook 的功能部分.

（Ⅰ）信任关系图(Matryoshka)

是一种逻辑关系图，将一些具有信任关系的节点组织在一起，分布在一组同心圆上. 每个用户进入系统后，都以自己为中心节点，建立并维护这样一个关系图. 中心节点外第一层节点都与中心节点相互信任. 第一层节点加密存储了中心节点的用户数据，因此将其称为镜像节点(image node). 第一层节点的信任节点都分布在第二层，以外各层都被内层节点所信任. 用户想要向中心节点发送消息，都要从信

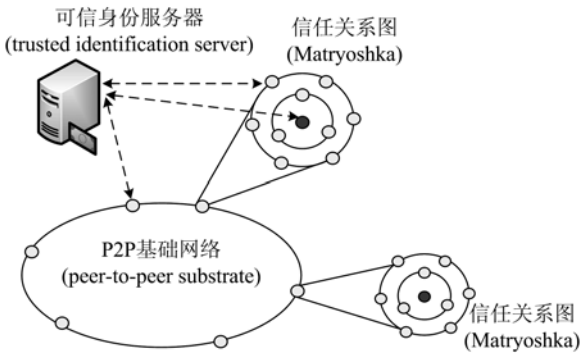

图 3　Safebook 系统结构示意图

Fig. 3　System architecture of Safebook

任关系图的最外层节点开始，一层一层向内传递. 这样，消息的传递都发生在两两信任的节点之间，但路径上的节点不必都是目标节点的信任节点，而且，每个节点的关系列表作为私密信息，不能被自己以外的节点所知，这样外部节点无法猜测数据传输的真正路径.

（Ⅱ）P2P 基础网络(peer-to-peer substrate)

包含所有节点. 这些节点通过特定的协议，以分布式哈希表(DHT，distributed Hash table)的形式组织在一起. 在这一层次中，每个节点使用唯一假名作为分布式哈希表中的标识. Kademlia 协议规定，每个节点维护 160 个 k-buckets，每个 k-bucket 包含一系列三元组：<IP address，Port，Node ID>，节点查找和新节点加入都要通过这个三元组来完成. Safebook 中以可信身份服务器提供的假名区分不同节点，因此，三元组为 < Node IP，Port，Pseudonym>. 此外，还要将<key，value>对注册存储在一些节点中，此处 key 是用户信息中某些属性的散列运算值，或节点标识符，value 是要存储的真正信息.

（Ⅲ）可信身份服务器(trusted identification server)

扮演可信第三方的角色，每个进入网络的用户都必须通过可信身份服务器获得许可，服务器为用户生成唯一假名、唯一节点标识符以及对这两种信息的真实性证明. TIS 也要在 DHT 中注册，这样，一个没有经过许可的非法用户是无法与 TIS 通信的.

Safebook 的安全优势有如下几点：

（Ⅰ）认证性

①新用户入网都要建立在与注册用户的信任基础之上；

②要向 TIS 提供身份证明，以获得认证授权，抵抗假冒攻击.

（Ⅱ）私密性、访问控制及数据完整性

①严格的信任关系管理，数据传输在信任链路上进行，身份信息只能在足够信任的节点间共享，保证匿名特性；

②在两个层次上采用公钥加密方案，既保证数据访问有严格的权限控制，又能保证每一跳信息传输的保密性.

（Ⅲ）系统可用性

①加强节点间合作，排除不信任节点的恶意行为；

②入口节点位置(以节点 IP 地址标识)通过 DHT 协议的查询操作获得，防止错误路由、黑洞攻击等.

3.4　Persona

当社交网络被越来越多的人所接受时，牵涉到的用户数据量也就越来越庞大，因此，用户数据的分组管理成为必要的使用需求. 所谓分组管理是指，通过用户指定或自由组合，联系人被分为不同的群组，每个群组对应的数据和消息只能由用户和群组内成员访问. 这样的分组管理方式可以通过传统的对称加密方案实现，但是，其密钥管理复杂，也增大了数据存储的冗余度，同时，无法抵御合谋攻击.

针对这样的问题，文献[28]将基于属性的加密(attribute based encryption，ABE)[29]和传统的公钥加密相结合，并提供自动化的密钥管理方案，设计了由用户决定访问策略的无中心系统，即 Persona 方案，允许用户将个人数据在中间媒介上加密存储，并且不要求中间媒介一定被用户所信任.

为了应用 ABE 算法，系统中的每个用户都要生成一个 ABE 公钥(APK，ABE public key)和一个 ABE 主密钥(AMSK，ABE master secret key). 对于每个联系人，为其分配 ABE 私钥(ASK，ABE secret key)，ASK 与联系人所在群组的相关属性对应.

在 ABE 算法中，每一次加密都要对应特定的“访问策略”. 例如，用户 A 加密一组数据，并对应访问策略<“同学”或“同事”>，这里，“同学”和“同事”都是属性，而不是群组，那么具有“同学”或“同事”两个属性其中之一的联系人都可以对加密信息进

行解密.而如果访问策略是<“同学”和“同事”>,那么只有同时具有“同学”和“同事”两个属性的人才能对加密信息进行解密.另外,所有能够获得用户ABE公钥的联系人都可以建立访问策略并加密数据,也就是可以创建新群组.该方案有两点主要优势:

①用户和联系人之间或联系人之间进行信息交互时没有必要获得详细的属性列表,只要在不同的群组中选用不同的访问策略,就可以控制对于信息的访问权限.

②群组的创建灵活,可由用户本身创建,也可由联系人创建.例如,用户A在自己的页面上发布了一条供“同学”这个群组阅读的消息,联系人B对这条信息进行回复,但回复的内容只想让“同学和同事”这个群组阅读,如果利用ABE算法,那么B只需将访问策略加以修改,就可以在逻辑上成立一个新的群组.如果通过传统的加密方式,B只能通过A的帮助重新建立群组.

3.5 一种便于群组撤销的隐私保护方案

文献[30]提出了一种便于群组撤销的隐私保护方案.该方案适用于用户私密信息存储在第三方网站的情况下的数据隐私保密和访问控制.同时,提高了数据搜索效率,也为频繁变化的用户群组关系提供了动态的群组建立和撤销方案.

文献[30]和文献[28]的两种方案都提供了群组化的管理方案.文献[28]采用了基于属性的加密,其优势是使得群组的组合、用户关系的建立较为灵活,但是其算法复杂度较高,也没有合适的群组撤销方案,不适用于用户数量较多,且群组关系变化较为频繁的应用场景.文献[30]的方案提出了基于角色的(role-based)加密方案,即每个用户一次只能分配一个角色,同时通过广播加密、支持关键字搜索的公钥加密等方案提高了群组建立、撤销以及数据搜索和获取的效率.文献[30]涉及的主要理论有:

(Ⅰ)基于身份的加密方式(IBE,identity-based encryption)[31]

采用该加密方式可以建立安全的通信架构并提高搜索效率.

(Ⅱ)广播加密(BE,broadcast encryption)[32]

这种加密方案允许中心用户将加密数据存储或转发,但只有特定权限的一组用户可以进行解密.广播加密主要由3步完成:

①建立(setup):针对某个用户 $u\in U$(U表示具有某个角色的用户集合),对于其身份标识符或者公钥,产生其密钥 $T_u\in T$(T表示一个密钥空间).

②广播(broadcast):指定撤销用户集合 R 和解密密钥 K,同时生成广播密文 C,C 中包含 K.

③解密(decrypt):用户 u 提供 T_u,获取在密文 C 中加密过的密钥 K,如果用户 u 是撤销用户集合 R 中的一员,那么,该用户则无法完成解密步骤.

采用广播加密可以提供较高效率的群组建立和撤销.例如,中心用户建立群组“同事”,即为一部分联系人分配“同事”这个角色,对于处于“同事”群组中联系人 u,中心用户为每个处于该群组的联系人分配不同的密钥 T_u(该密钥与 u 唯一对应,也与相应角色对应),并为该群组分配随机产生的解密密钥 K,用户 u 只有提供了 T_u 才能获取 K,进而对群组数据进行解密.如果中心用户要将 u 从“同事”群组中撤销,那么 u 被分配至撤销用户集合 R 中,相应的,用户 u 对应的 T_u 也失去作用,同时,中心用户为群组重新分配随机密钥,此时,如果 u 提供原来的 T_u 将无法获取新的群组密钥,无法完成解密.

(Ⅲ)带关键字搜索的公钥加密(PEKS,public key encryption with keyword search)[33]

在PEKS中,数据经过接收者的公钥加密后存储在远端服务器上,接收者自己选择关键字并计算关键字门限值,在接受者向服务器请求获取数据时,提供关键字门限值,服务器在加密数据中进行查找,只有包含关键字的内容才会被提供给接收者.采用PEKS加密方式可以提高数据的搜索和获取效率.

3.6 其他安全社交网络解决方案

本文前几个小节描述了多种典型的社交网络安全解决方案,除此之外,还有众多研究成果从不同的角度,对社交网络的安全应用加以保护.

文献[34]提到了社交网站应用过程中的“非对称设置”问题.所谓“非对称设置”是指用户对自己的私密信息设置权限保护,使得除指定联系人外,其他用户无法访问,但这些指定联系人并没有做相应的安全设置,这样,用户私密信息就会通过联系人的个人页面泄漏出去.针对这样的问题,文献[34]提出基于对称设置的隐私保护方案.文献[35]关注社交网络中用户位置及其发布内容的关系,针对基于位置的服务所带来的新安全隐患提出新环境下的安全解决方案.文献[36]提出一种可扩展的、以用户行为为中心的访问控制框架,通过属性控制、策略控制、关

系控制和会话控制等，提供高效、可用、可随需要变化的访问控制方案. 文献[37]认为社交网络是不同个体、群体、组织、网站及数据处理单元的关系映射和信息交互，因此，提出基于多方合作的社交网络隐私保护方案. 文献[38-39]着重考虑社交网络中数据大规模发布后邻居节点通过获取部分个人本地信息就可以轻松实施威胁的问题，并提出了相应解决方案.

4　安全社交网络研究方向展望

随着社交网络应用的不断兴起，其安全问题也日益突出，在对于安全社交网络解决方案的研究过程中出现了很多的开放性问题. 本文的目的在于，围绕社交网络的安全问题及已经存在的安全社交网络解决方案，把握安全社交网络研究领域未来的发展方向，具体地，可以总结为如下几个方面：

（Ⅰ）无中心社交网络架构实现方案

针对现有社交网络用户数据存储集中度过高的问题，以 P2P 网络作为底层社交网络节点的组织形式，研究社交网络无中心化的解决方案，目的在于去除中心服务器，以一种分布式的方案存储和传输数据.

（Ⅱ）数据的安全存储和加密传输方案

通过网络架构的无中心化，达到了数据分布式存储的目的，但数据保密性依然应当受到重视.

（Ⅲ）群组化信息共享方案

结合用户的不同需求场景，在基于属性和基于角色的访问控制策略基础上，充分利用用户好友之间的信任关系，研究便于用户信息群组化管理和用户自定义访问策略的信息共享方案，目的在于保证不同的用户信息只能被特定的人群访问，保证私密性.

（Ⅳ）安全身份认证方案.

针对传统的用户名加密码的登录方式容易出现密码被盗的情况，结合新型认证方式，研究安全的身份认证方案，保证用户进入系统时的合法身份，提供最基本的安全防护，使得攻击者难以盗取用户身份和非法登录系统.

（Ⅴ）无线社交网络安全问题的研究及解决

种类繁多的移动终端，特别是智能终端设备性能的不断提高，足以满足无线网络接入和第三方软件运行的需求. 同时，通过移动终端随时随地接入网络，享受服务，进一步推进了用户使用社交网络的实时性和方便性，因此，移动社交网络的普遍应用也是必然趋势，但是由于无线网络的开放特性，使得移动社交网络面临着更多更复杂的安全隐患.

（Ⅵ）社交网络和云计算结合下的资源共享模式及其安全问题的解决

云计算和社交网络是目前迅速发展的两种网络应用模式. 社交网络反映了用户之间的复杂关系，同时涉及大量的数据存储，云计算服务很重要的一个方面恰恰是数据存储，这使得社交网络和云计算相结合并产生新的应用模式成为一种发展趋势. 目前，已有学者提出“社交云(social cloud)”的概念[40]，并指出其中的安全问题. 因此，设计基于社交网络的云计算应用架构，分析其中的安全问题，并提出安全、可信的数据存储和共享机制也将是安全社交网络研究领域的新热点.

5　结论

本文首先介绍了社交网络的发展历史和应用现状，并在分析社交网络安全现状和安全问题的基础上，介绍了几种现有的较为完整的安全解决方案. 这几种解决方案都以保护用户隐私、加强访问控制和提高数据访问效率为目标，针对不同应用场景提供了较为完善的系统架构. 其中，VisualSec 以 ID-based 加密理论为基础，提出以图片信息为身份标识的数据加密方案；Social-K 提出了一种移动社交网络隐私保护方案；Safebook 提供无中心的社交网络架构，并结合 DHT 算法在保证数据安全存储、转发和访问控制的基础上提高访问效率；Persona 以及另外一种便于群组撤销的隐私保护方案有类似之处，提供了基于角色或群组的数据访问控制方案，不同之处在于，前者基于 ABE 算法，没有提供群组撤销方案，而后者提出基于角色的方案，并采用了广播加密、关键字可搜索的公钥加密等理论，提高数据查询效率. 同时，简要介绍了其他 5 种针对不同问题的安全社交网络解决方案. 最后，对安全社交网络的研究热点和研究方向予以归纳及展望.

参考文献(References)

[1] Boyed D, Ellison N. Social network sites: Definition, history, and scholarship[J]. Journal of Computer-Mediated Communication, 2008, 13(1): 201-230.

[2] Ahn G, Shehab M, Syuicciarini A. Security and privacy in social networks [J]. IEEE Internet Computing, 2011, 15(3): 10-12.

[3] Nagy J, Pecho P. Social network security [C]// Proceedings of the 3rd IEEE International Conference on Emerging Security Information, Systems and Technologies. Athens, Greece: IEEE Computer Society, 2009: 321-325.

[4] Zhang C, Sun J Y, Zhu X Y, et al. Privacy and security for online social networks: Challenges and opportunities [J]. IEEE Network, 2010, 24(4): 13-18.

[5] Luo W M, Liu J B, Liu J, et al. An analysis of security in social networks[C]// Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing. Chengdu, China: IEEE Computer Society, 2009: 648-651.

[6] Douglis F. It's all about the (social) network [J]. IEEE Internet Computing, 2010, 14(1): 4-6.

[7] Weaver A C, Morrison B B. Social networking [J]. IEEE Computer Magazine, 2008, 41(2): 97-100.

[8] Irani D, Webb S, Pu C, et al. Modeling unintended personal-information leakage from multiple online social networks[J]. IEEE Internet Computing, 2011, 15(3): 13-19.

[9] Limsaiprom P, Tantatsanawong P. Social network anomaly and attack patterns analysis[C]//Proceedings of the 6th IEEE International Conference on Networked Computing. Heidelberg, Germany: IEEE Press, 2010: 11-13.

[10] Hogben G. Security Issues and Recommendations for Online Social Networks [R/OL]. European Network and Information Security Agency, 2007 [2011-04-20]. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

[11] Hogben G. Security issues in the future of social networking[R/OL]. W3C Workshop on the Future of Social Networking, 2009 [2011-04-20]. http://www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf.

[12] Choi J Y, Neve W D, Plataniotis K N, et al. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks [J]. IEEE Transactions on Multimedia, 2011, 13(3): 14-28.

[13] Poppe R. Scalable face labeling in online social networks [C]// IEEE International Conference on Automatic Face & Gesture Recognition and Workshops. California, USA: IEEE Press, 2011: 566-571.

[14] Gao Y, Deng L W, Kuzmanovic A, et al. Internet cache pollution attacks and countermeasures [C]// Proceedings of the 14th IEEE International Conference on Network Protocols. California, USA: IEEE Press, 2006: 54-64.

[15] Jagatic T, Johnson N, Jakobsson M, et al. Social phishing [J]. Communications of the ACM, 2007, 50(3): 94-100.

[16] Douceur J R. The sybil attack[J]. Lecture Notes in Computer Science, 2002, 2 429: 251-260.

[17] Maheshwari R, Gao J, Das S R. Detecting wormhole attacks in wireless networks using connectivity information[C]//Proceedings of INFOCOM'07: 26th IEEE International Conference on Computer Communications. Anchorage, AK: IEEE Press, 2007: 107-115.

[18] Ge M, Lam K, Wang X Q, et al. VisualSec: A secure message delivery scheme for online social networks based on profile images [C]// Proceedings of GLOBECOM'09: Global Telecommunications Conference. HI, USA: IEEE Press, 2009: 1-6.

[19] Shamir A. Identity-based cryptosystems and signature schemes [J]. Lecture Notes in Computer Science, 1985, 196: 47-53.

[20] Beach A, Gartrell M, Han R. Social-K: Real-time K-anonymity guarantees for social network applications [C]// Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops. Mannheim, Germany: IEEE Press, 2010: 600-606.

[21] Beach A, Gartrell M, Ray B, et al. Secure SocialAware: A Security Framework for Mobile Social Networking Applications: [R]. Boulder, CO, USA: University of Colorado at Boulder, 2009: Technical Report CU-CS-1054-09.

[22] Beach A, Gartrell M, Han R. Solutions to security and privacy issues in mobile social networking [C]// Proceedings of the International Conference on Computational Science and Engineering. Vancouver, BC: IEEE Press, 2009: 1 036-1 042.

[23] Sweeney L. K-anonymity: A model for protecting privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.

[24] Cutillo L A, Molva R, Strufe T. Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network[C]// IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops. Kos, Greece: IEEE Press, 2009: 1-6.

[25] Cutillo L A, Molva R, Strufe T. Privacy preserving social networking through decentralization [C]// Proceedings of the 6th International Conference on

Wireless On-Demand Network Systems and Services. Snowbird, UT: IEEE Press 2009: 145-152.

[26] Cutillo L A, Molva R, Strufe T. Safebook: A privacy-preserving online social network leveraging on real-life trust[J]. IEEE Communications Magazine, 2009, 47(12): 94-101.

[27] Maymounkov P, Mazieres D. Kademlia: A Peer-to-peer information system based on the XOR metric[J]. Lecture Notes in Computer Science, 2002, 2 429: 53-65.

[28] Baden R, Bender A, Spring N, et al. Persona: An online social network with user-defined privacy[C]// Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication. Barcelona, Spain: ACM, 2009: 135-146.

[29] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy. California, USA: IEEE Press, 2007: 321-334.

[30] Sun J Y, Zhu X Y, Fang Y G. A privacy-preserving scheme for online social networks with efficient revocation[C]// Proceedings of INFOCOM 2010. San Diego, USA: IEEE Press, 2010: 1-9.

[31] Boneh D, Franklin M. Identity-base encryption from the weil pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[32] Fiat A, Naor M. Broadcast encryption[J]. Lecture Notes in Computer Science, 1994, 773: 480-491.

[33] Boneh D, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search[J]. Lecture Notes in Computer Science, 2004, 3 027: 506-522.

[34] Tang C, Wang Y G, Xiong H, et al. Need for symmetry: Addressing privacy risks in online social networks[C]// Proceedings of IEEE International Conference on Advanced Information Networking and Applications. Biopolis, Singapore: IEEE Press, 2011: 22-25.

[35] Vicente C, Freni D, Bettini C, et al. Location-related privacy in geo-social networks[J]. IEEE Internet Computing, 2011, 15(3): 20-27.

[36] Park J, Sandhu R, Cheng Y. User-activity-centric framework for access control in online social networks[J]. IEEE Internet Computing, 2011(99): 1-9.

[37] Zhan J. Secure collaborative social networks[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2010, 40(6): 682-689.

[38] Singh L, Schramm C. Identifying similar neighborhood structures in private social networks[C]// Proceedings of IEEE International Conference on Data Mining Workshops. Sydney, Australia: IEEE Press, 2010: 507-516.

[39] Tripathy B K, Panda G K. A new approach to manage security against neighborhood attacks in social networks[C]// Proceedings of IEEE International Conference on Advances in Social Networks Analysis and Mining. Odense, Denmark: IEEE Press, 2010: 264-269.

[40] Chard K, Caton K, Rana O, et al. Social cloud: Cloud computing in social networks[C]// Proceedings of the 3rd IEEE International Conference on Cloud Computing. Florida, USA: IEEE Press, 2010: 99-106.