LBS 系统中的安全性研究

戴忠华[1] 彭 勇[1] 赵天宇[2]

(1. 中国信息安全评测中心,北京 100085;2. 北京邮电大学,北京 100876)

摘要: LBS(基于位置服务)是利用移动用户的位置信息,为用户提供的一种新型的增值服务。用户位置信息具有天然的敏感性,加之目前专门针对LBS的政策法规的缺位,如何防止用户位置信息的泄露便成为一个亟待解决的问题。对此,本文通过分析LBS系统的架构、服务流程来阐述目前已经应用于LBS系统的安全隐私保护措施,以此为基础尝试寻找目前LBS系统存在的安全隐患。本文提出了3个目前仍然存在的安全隐患,分析了这些隐患可能带来的严重后果,进而提出一系列的解决这些安全隐患的具体方法。本文列举的提升LBS系统安全性、隐私性的方法,有些需要占用运营商和SP的大量资源,有些则牺牲了定位的准确性。

关键词: 基于位置服务(LBS);安全性;隐私性

A Survey of security for LBS system

DAI Zhonghua[1], *PENG Yong*[1], *ZHAO Tianyu*[2]

(1. China Information Technology Security Evaluation Center, Beijing 100085, China;
2. Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: LBS (Location Based Service) is a new kind of value-added service provided for users by using location information of UEs. The natural sensitivity of location information, together with the absence of policies and regulations especially for LBS, has made it seriously important to find a method to prevent the disclosure of location information. To deal with this, in this paper, we introduce current protection measures in security and privacy through the analysis of the construction and service progress of LBS systems, and try to find some security risks in current LBS systems. We come up with 3 security risks in existence and the serious consequences of them, and then we introduce a series of methods to solve these problems. Some of the methods upgrading the security and privacy stated in this paper will occupy large amount of resources of operators and SPs, while some of them will decrease the accuracy of localization.

Key words: Key words: LBS; security; privacy

收稿日期: 2011-05-10

基金项目: 国家自然科学基金重点项目(90818021)

作者简介: 戴忠华(1978—),男(汉),江苏,助理研究员

E-mail: zhonghuadai@itsec.gov.cn

LBS(基于位置服务)是通过 GSM、3G 网络获取移动终端用户的位置信息(如经纬度坐标),在电子地图平台的支持下,为用户提供相应服务的一种增值服务。开通了基于位置服务,终端用户就可以方便地获知自己或他人目前所处的位置[1,2,3]。由于 LBS 业务的迅速发展,用户数量的激增,如何保障整个系统的安全和用户的隐私不受侵犯便成为用户和政府关注的重要问题。研究表明,大约 24% 的用户都非常在意位置对他们安全的影响,而大量用户位置信息的泄露也可能会威胁到社会的稳定和国家的安全[4]。

尽管目前 LBS 系统采取了许多提升系统安全性和保护用户隐私的手段,例如运营商对于用户和服务提供商的鉴权、用户自身的隐私设置、用户伪号码使用等,但是仍然存在诸如敏感地区信息泄露、用户自身位置泄露等安全隐患。

本文分析了 LBS 的逻辑结构和服务流程;分析了 LBS 的客户端鉴权、发起方鉴权、用户签约信息监测、用户标识保护的具体过程;在上述的分析之后,找出当下 LBS 存在的安全隐患;最后,提出提升 LBS 安全性、私密性的具体方法。

1 LBS 的安全现状

如图 1 所示,LBS 系统在逻辑上可分为 3 部分[5]:LBS Client(LBS 服务提供商,即 SP)、LSP(位置服务平台)和 Target MS(目标移动台)。SP 允许 LBS 用户通过多种方式接入,如短消息、WAP、WEB 和语音等。在接到用户的业务请求后,SP 首先对用户的身份进行鉴权,检查用户是否具备使用该业务的资格。之后 SP 将定位请求发给移动运营商提供的 LSP。LSP 先要对 SP 的身份进行鉴权(包括确认 SP 是否在系统中注册、SP 提出定位请求的类型、SP 是否欠费等);而后结合 Target MS 在 LSP 中注册的隐私保护信息来决定是否允许此次定位请求。若定位请求被允许,则实施定位,并将定位结果发送回 SP。SP 根据 LSP 提供的 Target MS 的位置信息为用户提供相应服务[6-7]。

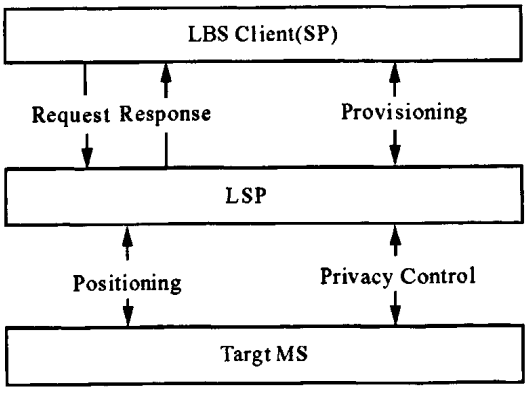

图 1 LBS 系统逻辑结构及定位流程

根据上面对于LBS系统的逻辑描述，LBS系统中目前已采取的安全隐私保护措施有如下几项：

1. SP对于LBS用户的鉴权

用户在使用SP提供的各种LBS业务之前，要在SP中注册自己的个人信息（如设置用户名、密码或使用自己的电话号码注册，同时SP还要对用户的资格进行审核）。SP还要管理每个用户的业务权限（允许使用哪些业务，禁止使用哪些业务）。使用LBS业务时，SP根据用户的注册信息和业务权限来决定是否为该用户提供服务。

但是这些仅仅是移动运营商对于SP的要求（必须具备这些机制才与之签约合作），SP是否能够充分执行则是未知数。而就目前的情况来看，SP为了抢占市场，扩大用户群，往往没有采用严格的用户资格审核机制和用户业务权限机制。同时，一些非法的SP本身就扮演了窃取用户隐私的角色，关于这一点将在文章后面具体说明。

2. LSP对于SP的鉴权

只有预先在运营商注册过的SP才能接入LSP平台。在提供用户位置数据之前，LSP必须鉴别SP的身份、判断此次服务的业务类型、了解SP具有的权限。SP的权限有高有低，其中最高的是紧急服务类业务，它可以使LSP在不考虑用户隐私设置的情况下，直接定位用户，并将结果返回给SP。然而权限较低的增值服务类业务则需要考虑用户隐私设置。

3. 用户隐私设置

用户可以随时更改存储于归属地LSP的LBS业务相关数据。其中包括黑名单（禁止向名单中的SP发送位置信息）、白名单（可在不被提示的情况下向名单中的SP发送位置信息）、灰名单（向名单中的SP发送位置信息前询问用户）、时间范围（在一定的时间内可以被定位）、地域范围（处于一定的位置时将不能被定为）等。

另外，在用户要求的情况下，LSP应可以在定位结束后，先将定位结果发送给移动台，再由移动台用户决定是否将该位置信息发送给SP。

4. 用户伪号码的使用

为了保护用户的隐私，SP和LSP之间的通信使用的是用户伪号码，而不是IMSI或MSISDN。在移动台的本地环境中设有PMD（Pseudonym mediation device），专门负责伪号码和IMSI之间的转换。目前IMSI和伪号码是一一对应的，这位非法SP挖掘用户隐私提供了便利，关于这一点将在文章后面具体说明。

5. 网络安全

在无线传输中的安全由现有的GPRS或GSM提供的安全机制来保障；在IP网上，LSP对外开放，其所有服务器均应安装安全防护系统（例如：防火墙设备、防

病毒防黑客系统等);对于和第三方合作的外部增值应用平台,应具备验证、授权和加密的功能以保证系统的安全性。

2 LBS的安全隐患分析

虽然目前的LBS系统中的鉴权机制已非常完善,并且能够通过传输过程中的加密、每个服务器安装防火墙等措施保障用户的位置信息不被第三方窃取和篡改,但是相关政策法规的缺乏导致SP行为不规范和伪号码同IMSI的一一对应关系等LBS系统中的不足还是为不法分子窃取用户的位置隐私,甚至进一步危害用户人身财产安全的可乘之机。下面是在目前的LBS系统中可能发生的由于安全隐患带来的危害:

1. 敏感地区信息泄露

比如,国外反动组织预先建立一个SP,让所有位于我国的间谍在该SP上注册。在间谍到达敏感地区时,便可以使用类似于时下非常流行的"报到"业务在SP上"报到",将自己目前所在敏感地点的坐标传送给SP。如此以来,我国的敏感地点的坐标便能轻易地被发动组织掌握,危害国家安全。

目前,国家对于提供"报到"业务的SP(特别是国外的SP)采取了更加严格的审核措施。例如著名的美国LBS社交网站Foursquare,因为频频有用户在中国的敏感区域报到,中国政府便利用GFW将其屏蔽。但是,如若换一种形式,不是让间谍在敏感区域"报到",而是通过使用POI业务(例如搜索其附近的餐厅、旅馆或者加油站等),变相地让SP获知间谍所在区域坐标,则中国会因为拿不出相应的证据而无法将该SP屏蔽。

2. 用户自身位置泄露

目前LBS在无线传输过程中的安全由现有的GPRS、GSM(3G网络)所提供的机制保障,并且在IP网上,所有服务器都安装了防护系统(如防火墙设备、防病毒黑客系统)。

这种安全措施显然是不够的,一旦发现现有的机制漏洞,那么就可以获得在LBS在定位过程中没有被加密的数据。例如:在处理紧急业务时,运营商与LBS服务提供商之间的信息交互直接采用移动台的MSISDN,而不是伪号码。若这种信息被他人截获,很可能就能掌握用户的MSISDN和其对应的地理方位。

另外,目前有很多LBS并不是通过运营商提供的。例如Google提供的Geo-locationAPI服务。该服务要求终端的应用按照Google所规定的格式,通过分组交换网向Google的服务器发送GPS定位结果(经纬度),基站信息(包括Cell-id、LAC、信号强度等),Wifi接入信息(包括MAC地址、信号强度等)三者中的一个或多个至服务器中,经过计算,而后再返回经纬度、海拔、精确度、地址等信息到手

机中。

在整个消息传递过程中，没有对与信息的传输进行加密。这显然也会使得服务用户面临暴露自身位置隐私的风险。

3. 用户身份泄露

假如不法分子在已知某重要人物的住址之后，建立一个 SP，持续观察所有来自该住址的定位请求，若发现所有来自此处的定位请求都来自同一个用户，那么就可以断定该用户就是这位重要人物或者与其亲密的人。由于伪号码和用户 IMSI 的一一对应关系便可利用已知的用户伪号码持续对该用户进行跟踪，威胁重要任务或与其亲密的人的安全。

又比如某保安公司在运钞时使用 LBS 对其运钞车的行进路线进行监控，而犯罪团伙通过踩点了解到该保安公司的运钞计划的一部分（如：在每星期一的时间段 T 内从 A 银行总行至 B 支行，以及运输的具体路线），那么他们就可以搭建一个 SP，在时间段 T 内监控从 A 行到 B 支行的位置请 LBS 求信号。如果在时间段 T 内所有的请求都来自同一个用户，那么犯罪团伙就可以确认该用户即为该保安公司的运钞车，便可以对其进行实时的监控。

3 LBS 安全改进措施

针对目前 LBS 系统存在的敏感地区信息泄露、用户自身位置泄露和用户身份泄露的安全隐患，国内外研究人员针对 LBS 的安全隐患提出了各种各样的改进意见：冗余查询机制能够保障用户自身位置信息安全；PROBE 系统杜绝了不法分子通过构建 SP，提供 POI 业务获取敏感地区信息的可能；SpaceTwist 能够有效阻止提供 POI 业务的 SP 获知用户位置；K-Anonymity（K-匿名）保护机制可以从根本上防止用户身份泄露；PIR 框架在不引入第三方平台的情况下，可以解决现有的所有安全问题。此外，本文也提出了一些在没有 LSP 参与 LBS 中的安全保障措施。

3.1 运营商参与的 LBS 业务的安全改进措施

1. 冗余查询机制

引入由 H Kido 在[8]中提出冗余查询机制可以使得 SP 无法寻找到用户的真实位置。LSP 在收到 User 的 LBS 业务请求后，使用伪号码向 SP 提出用户 LBS 业务请求时，可以在一段时间内发送多个同一 User（具有同样伪号码，在处理紧急业务时则为同一 IMSI）的请求。这些请求得到响应后，LSP 对于其中用户确实需要的那个定位请求按照正常的定位流程进行定位；对于其余的冗余请求则采取随机的方式向 SP 发送一些随机位置。最后 SP 将用户 LBS 业务结果返回给 LSP

后,LSP 将其中 User 的 LBS 业务请求的响应发回给用户,丢弃其余的结果。

该机制不需要引入第三方平台,简单可行。但是无法保证用户身份不会被泄露(若 SP 已知用户 B 在 A 点,A 点发出定位请求的用户很大部分是 B,则 SP 就可以确定用户的伪号码),同时此方法还会占用 LSP 和 SP 的大量资源。

2. PROBE 系统

通过引入 M Damiani 在[9]中提出的 PROBE 系统,可以防止在 POI 应用中泄露敏感区域的具体位置。在第三方平台的 PROBE 系统中,地图被分为许多正方形。LSP 向 SP 传送定位结果前,先经过 PROBE 系统,系统向 SP 发送的不再是具体坐标,而是一定的坐标范围。如图 2 所示,若用户位于敏感区域 H,那么 PROBE 系统向 SP 发送的坐标范围就是图中粗框子的范围,而不是具体的灰色格子的范围。其中 OR1 和 OR2 中 H 占发送位置区域范围的比例均小于 44%,因而可以保证用户位于敏感区域的精确坐标被 SP 掌握。

该方式需要引入第三方平台,建立庞大的数据库系统,增加了移动运营商的运营成本。另外,PROBE 系统同冗余查询机制一样,无法保证用户的身份不会被泄露。

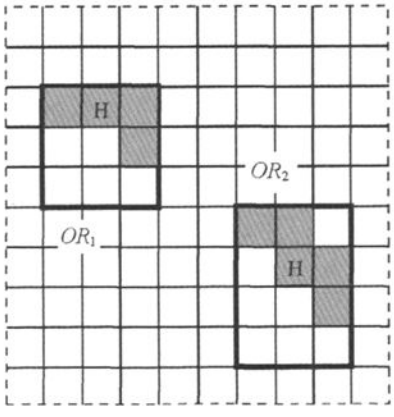

图 2 PROBE 系统

3. SpaceTwist 机制

M L Yiu 在[10]中提出的 SpaceTwist 机制可以防止 POI 应用中用户位置的泄露。该机制需要引入值得信任的第三方平台。LSP 收到 SP 的 LBS 业务请求并定位用户后,并不是把用户位置信息直接发送给 SP,而是将用户的所在位置坐标发送给第三方平台。之后第三方平台向 SP 发送的坐标并不是图 3 里 Initial Phase(初始阶段)中用叉子表示的用户的真实坐标,而是一个名为 anchor 的虚假坐标。

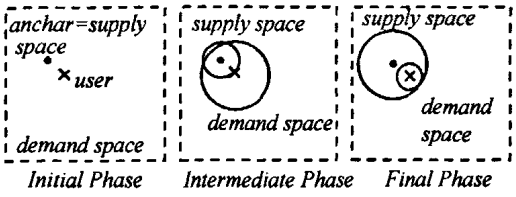

图 3 SpaceTwist 机制时序图

在 Intermediate Phase(中间阶段)中 SP 通过其服务器存储的地理信息找寻 anchor 附近的 POI,并不断扩大其搜索 POI 的范围(即 Supply Space)。Demand Space 是第三方平台根据用户所需的 QoS 制定的实际需求的 POI 搜索范围。在 Final Phase(结束阶段)中 Supply Space 将 Demand Space 完全覆盖,此时第三方平台便可以将搜索到的 POI 发回给 LSP,LSP 将定位结果发回给用户。

通过这种方式,使得 SP 无法掌握用户真实的地理位置。但是会加重 SP 的运算开销,延长服务时间。同时第三方平台的引入也增加了运营商的运营成本。另外,SpaceTwist 机制也无法保证用户的身份不会被泄露。

4. K-Anonymity(K-匿名)保护

Mokbel M F 在[11]中提出的 K-Anonymity 保护方式不但可以防止用户位置泄露,还可以防止用户身份泄露。K-匿名保护需要引入一个集中式的第三方中间件层:位置匿名器。当用户向服务器发送 LBS 服务请求时,先把位置信息发送给位置匿名器。匿名器将用户的坐标位置泛化为一个具有 K 匿名性质的区域。该区域满足一定的面积大小,而且区域内有至少 K 个用户,用户的身份在该区域内被识别出来的概率仅为 1/K。采用该方式时,SP 应添加一个查询处理器,它能够快速地处理空间区域的查询,找出所有的候选结果,并返回给用户,让用户从中选择一个最优的。它还保证返回给用户的结果候选集尽可能小,且包含了用户查询请求的正确结果。

虽然该方法考虑周全,能在很大程度上解决了位置隐私保护存在的问题,但在保护的同时也对 SP 的处理能力提出了更高的要求。另一方面,由于移动用户的位置信息是出于不断变化之中。位置变化了,位置匿名器产生的匿名区域也需要改变,同时服务器返回给用户的信息也需要改变。因此,服务器需要具有随时处理用户位置发生变化的能力。

5. PIR(Private Information Retrieaval)框架

G Ghinita 在[12]中提出了在 LBS 系统中引入 PIR 框架以增加其安全性的具体方法。

入 PIR 框架如图 4 所示,请求 $q(i)$是被加密的,谁都无法从 $q(i)$中解析出 i。并且 Client 可以通过 $r(X,q(i))$轻易地计算出 Xi。这样便实现了一个 Client 在不让 Server 知晓其请求数据的情况下秘密的获得信息的协议。

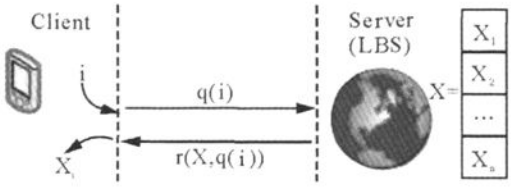

图 4 PIR 框架

通过引用这个框架 LSP 将每个 POI 的位置信息 p_i 作 Hilbert Curve 变换，得到 $H(p_i)$，将所有 $H(p_i)$的上传至 SP。这个变换的参数对 SP 保密；保障 SP 不能从 $H(p_i)$中经过运算得到 p_i。在 POI 查询过程中，LSP 首先根据用户的位置信息 u 计算出 $H(u)$，之后向 SP 请求最接近的 $H(p_i)$值。最后对于该数值做 H^{-1}变换，计算出 POI 的位置信息，并将其发回给用户。

这种方式不需要借助第三方平台，但是保证私密性则依赖于 Hilbert Curve 变换参数的大量选取和更新，而且这种服务方式不能保证能够提供准确的位置信息。

3.2 运营商未参与的 LBS 业务的安全改进措施

目前所提出的安全隐私保护措施主要是针对传统 LBS，即 SP、LSP 和 Target UE 三方参与的系统。随着云计算的发展，在没有 LSP 介入的情况下，Target UE 可以直接 SP 通信，获得导航、POI 查询、公交查询等 LBS 服务。针对此类 LBS，本文提出了如下一些安全保障措施。

以 Google 提供的 GeolocationAPI 为例，该服务要求终端的应用按照 Google 所规定的格式，发送 GPS 定位结果(经纬度)，基站信息(包括 Cell-id、LAC、信号强度等)，Wifi 接入信息(包括 MAC 地址、信号强度等)三者中的一个或多个至 Google 的服务器中，经过计算，返回经纬度、海拔、精确度、地址等信息到手机中。

因此即便是没有 GPS 或者 Wifi 功能的移动台，也可以通过提供目前所在小区的 Cell-id、LAC、信号强度等基本信息被定位。在目前移动台的操作系统的支持下，手机软件可以轻易地获得移动台的 Cell-id 等信息：诺基亚为程序开发人员提供例程，使得 Symbian 应用在获得证书的情况下，可以轻松获得当前移动台所在的 Cell-id；除此以外，通过 J2ME、RIL 等开发工具开发的应用程序也可以获得当前移动台 Cell-id、LAC 信息。这就为一些非法软件定位用户位置提供了便利，开发者可以将获取用户 Cell-id、LAC 以及信号强度等信息的代码隐藏在程序中，获知用户的大致位置，甚至通过以 Google 为例的第三方平台计算得到更为精确的位置。

对此，我国监管机构应该出台相应的政策，强制规定移动台中的应用在获取用户的 Cell-id 等信息时，要遵循一定的鉴权机制(如黑、白、灰名单，提示用户等)。

另外，移动台在与Google服务器通信过程中没有对信息进行加密，这就使得攻击者可能截获到用户所在的小区信息。因此Google可以使用用户的注册密码作为DES加密时使用的密钥，将信息进行加密。

4 结　论

本文首先通过分析LBS系统的架构、定位技术和服务流程来阐述目前LBS系统已经采取的安全隐私保护措施，这些措施包括SP对于LBS用户的鉴权、LSP对于SP的鉴权、用户隐私设置、用户伪号码的使用和网络安全；之后提出一些目前仍然存在的安全隐患以及这些隐患可能带来的严重后果，包括敏感地区信息泄露、用户自身位置泄露和用户身份泄露；而后针对这些安全隐患提出了一系列的提升LBS系统的安全性和隐私性的方法，并对于没有LSP参与的一类特殊的LBS系统提出了一些安全改进措施。本文列举的提升LBS系统安全性、隐私性的方法，有些需要占用运营商和SP的大量资源，有些则牺牲了定位的准确性。因此到底运营商会采取哪些方法，会不会诞生代价更小的方法，还需拭目以待。

参 考 文 献

[1] 谢彩香. LBS移动终端导航电子地图设计与实现 [D]. 济南：山东科技大学，2006.
Xie Caixiang. The design and realization of LBS electronic map for navigation in UEs [D]. Jinan: Shandong University of Science and Technology, 2006. (in Chinese)

[2] 孙国林，郭伟. 3G系统中定位服务的体系与结构 [J]. 广东通信技术，2001，21(11)：7-11.
Sun Guolin, Guo Wei. The system and structure of location service in 3G communication systems [J]. Guangdong Communication Technology, 2001, 21(11): 7-11. (in Chinese)

[3] 华云，龚耀寰，胡小川. 第三代移动通信系统中无线定位技术的实现 [J]. 系统工程与电子技术，2003，25(4)：397-400.
Hua Yun, Gong Yaohuan, Hu Xiaochuan. The realization of wireless localization technology in 3G communication systems [J]. System Engineering & Electronic Technology, 2003, 25(4): 397-400. (in Chinese)

[4] 石云. LBS系统的私密性研究 [J]. 信息安全与通信保密，2006，12(4)：67-69.
Shi Yun. A survey of privacy for LBS systems [J], Information Security & Communication Security, 2006, 12(4): 67-79. (in Chinese)

[5] QB-XX-XXX-200. V1.0.0.0-2002. 基于CELLID的位置业务(LBS)技术要求 [S]. 北京. 中国移动通信集团公司，2002.
QB-XX-XXX-200. V1. 0. 0. 0-2002. Technical requirements of LBS based on CELLID [S]. Beijing. China Mobile Communications Corporation, 2002. (in Chinese)

[6] 3GPP TS 22.071. V 10.0.0. Location Services (LCS), Stage 1 [S]. www.3gpp.org:

3GPP, 2011.

[7] 3GPP TS 23.271. V 10.2.0. Functional description of Location Services, Stage 2 [S]. www.3gpp.org: 3GPP, 2011.

[8] H Kido, Y Yanagisawa, T Satoh. An anonymous communication technique using dummies for location-based services [C]// International Conference on Pervasive Services (ICPS). Japan: IEEE Press, 2005: 88-97.

[9] M Damiani, E Bertino, C Silvestri. PROBE: an Obfuscation System for the Protection of Sensitive Location Information in LBS, Technical Report 2001-145 [R]. West Lafayette: CERIAS, 2008.

[10] M L Yiu, C Jensen, X Huang, H Lu. SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services [C]// International Conference on Data Engineering (ICDE). Cancun: IEEE Press, 2008: 366-375.

[11] Mokbel M F, Chow Chiyin, Aref W G. The New Casper: A Privacy-Aware Location-Based Database Server [C]// IEEE 23rd International Conference on Data Engineering (ICDE). China: IEEE Press, 2007: 1499.

[12] G Ghinita, P Kalnis, A Khoshgozaran, et al. Private Queries in Location Based Services: Anonymizers are not Necessary [C]// ACM SIGMOD international conference on Management of data. New York: ACM, 2008: 121-132.

LBS系统中的安全性研究

作者： 戴忠华， 彭勇， 赵天宇
作者单位： 戴忠华,彭勇(中国信息安全评测中心,北京 100085)， 赵天宇(北京邮电大学,北京 100876)