用户授权方式下的隐私数据保护和访问

Protection and Access of Private Data under Personal License

刘 松 (广东商学院信息学院 广州 510320)

摘要:P3P 为 Web 站点公布它们的在使用用户数据时的隐私策略提供了一种标准的方式。用户能够根据其制定的隐私策略来决定自己的响应方式。但这种机制不能监督当 Web 站点获得用户的数据后对其所采取的非法处理。基于此,本文提出了一种新的安全访问机制,称为个人数据许可证(PDL)机制,在此机制下,用户有权访问和修改其提供给 Web 站点的数据,同时,站点对用户数据的使用必须通过许可证的方式获得用户的授权。这种机制能保证用户数据不被非法滥用。

关键词:P3P 隐私策略 个人数据许可证

1 引言

当前,随着因特网的广泛使用,人们在获得极大便利的同时,在线隐私问题也越来越受到因特网用户的关注。主要包括:对安全存储和数据传递的关注;对未经用户授权的情况下收集个人数据的关注;对所收集和处理的数据的随意性将导致数据收集量的增加、数据库匹配和数据的二次使用问题的关注;对个人数据被传送到司法保护范围之外的地方使用的关注。显然,如果不能有效地解决上述问题,因特网的发展将受到极大的制约。

基于上述原因,万维网联盟(W3C)制定了 P3P 规范,该规范通过为隐私策略提供一个标准的可机读格式,以及一个能使 Web 浏览器自动读取和处理策略的协议来处理因特网用户所关心的数据隐私在线保护问题。在 P3P 规范中包含了一个描述数据处理方式的标准词汇表,以及一个用于描述所收集信息种类的基本数据模式,同时,P3P 规范也包含有用于请求和传输 P3P 策略的协议,该协议所基于的 HTTP 协议和 Web 浏览器用来与 Web 服务器进行通讯的 HTTP 协议相同。虽然 P3P 只涉及了保护隐私的一小部分,但它丰富了其它保护隐私的手段,包括法律、技术工具和隐私封印程序。随着 Microsoft 公司发布其支持 P3P 技术的 IE6 Web 浏览器之后,越来越多的 Web 站点,诸如新闻和信息站点、广告网、金融机构和政府机构等开始采用 P3P 技术。

2 隐私策略标准

公平信息执行准则是对个人数据保密的指导方针,按照其规定,Web 站点在制定其隐私策略时必须依照下面的隐私保护准则:

通告/知晓(Notice/Awareness):服务提供者(Web 站点)必须明确地告知它的客户其数据被使用的方式。

选择/同意(Choice/Consent):个人有权决定其数据是否被站点收集和使用。

访问/参与(Access/Participation):个人有权从数据控制者那里获取与己相关的数据,并有权要求对其进行删除、更正、补充完整或修正。

完整性/安全性(Integrity/Security):个人数据应当受到合理的安全保护措施的保护,以防止类似数据的丢失或未经许可的访问、破坏、使用、修改或公开的情况发生。

不幸的是,目前 P3P 规范仅满足通告和选择的原则,而不能满足参与和安全性原则。当用户将数据提供给 Web 站点后,他们不能对其进行访问和修改。另外,从 Web 站点所给出的 P3P 格式的隐私策略中,用户也无从知晓和监督其提供给 Web 站点的数据是否被非法滥用。

鉴于此,本文提出一种新的安全访问控制框架,通

过采用授权方式来对用户数据进行访问控制，使用户数据的使用始终处于用户的安全监督之下。

3 PDL 框架

简单来说，PDL 扮演了一个用户代理的角色，用来产生使用个人数据的许可证。如图 1 所示。

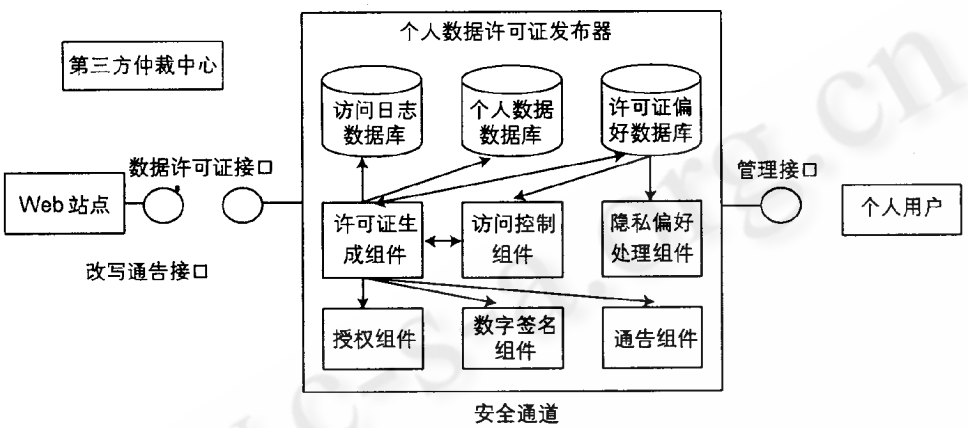

图 1　PDL 框架

当 Web 站点需要使用用户数据的时候，首先它要通过数据许可证接口（Data Licensing Interface）发出使用用户数据的许可证请求。许可证请求主要包括要使用的数据内容，使用目的和使用时间。

PDL 的核心部件是个人数据许可证发布器（Personal Data Licenser）. 它的具体实现可以是多种形式：它能以个人计算机中的软件代理的形式出现，也可以作为服务提供者所提供的一种服务，甚至可以出现在对等网中的各对等实体中。它的主要组成部分如图 1 所示。包括三个数据库：许可证发布器管理的个人数据库（Personal Data），个人在许可证中设置的隐私偏好数据库（Licensing Preferences），许可证请求日志数据库（Access Log）。另外还有 6 个功能组件，各部分的功能如下所示：

个人数据数据库：存放用户提供给 Web 站点的个人数据；

许可证偏好数据库：存放用户在许可证中设置的个人隐私偏好；

访问日志数据库：纪录许可证产生的情况以及对用户数据的访问情况；

许可证生成组件（Agreement Negotiator）：根据许可证隐私偏好数据库中设置的内容进行请求处理，产生使用用户数据的许可证。

访问控制组件（Access Control）：验证请求者对要使用数据的访问权限；

隐私偏好处理组件（Preferences Processor）：设置和处理用户的隐私偏好策略；

授权组件（Authentication）：验证请求者的身份；

数字签名组件（Digital Signature）：验证许可证的真实性，防止许可证内容被篡改；

通告组件（Notification）：产生用户和 Web 站点之间的通告信息；

如果许可证请求满足数据拥有者的隐私偏好设置，许可证生成组件将为被请求的用户数据产生一个使用许可证，为防止许可证的内容被篡改，并保证此许可证发布的真实性，许可证将被签上数据拥有者的数字签名。然后，许可证连同被请求的个人数据一起发送给请求者。同时，许可证请求和发布的许可证将被记录在访问日志中，以便让数据拥有者通过管理接口跟踪他们的使用。

为了保证通讯的安全性。PDL 通过授权组件来验证用户的身份，通过访问控制组件来验证请求者是否拥有对被请求数据的访问权限。

为了满足个人参与的原则，个人用户能够对其所发布的许可证内容进行修改。图 2 给出了一个改写通告的处理细节。如果个人用户 X 希望改写他发布给 Web 站点 Y 的许可证（包括对其中的条款进行增加、改写和删除），他可以让他的个人数据许可证发布器（Personal Data Licenser）通过改写通告接口发送一个改写请求 Ux 到 Web 站点。

收到一个改写请求后，Web 站点将给出它的响应

RUx,然后连同签有其私有密钥 Sky 的改写请求一并发回给提出改写请求的用户,采用签名机制能保证改写请求的真实性。

如果用户的改写请求在一定的时间内得不到有效地响应,这时,为了保证用户的权利,可引入第三方仲裁中心,用户可以将他们关于改写请求的申诉 COMPUx 发往仲裁中心。然后由仲裁中心来裁决 Web 站点延迟响应的原因:是由于 Web 站点的改写通告接口暂时出了问题,还是由于其怀有其它意图而故意忽略用户的请求。

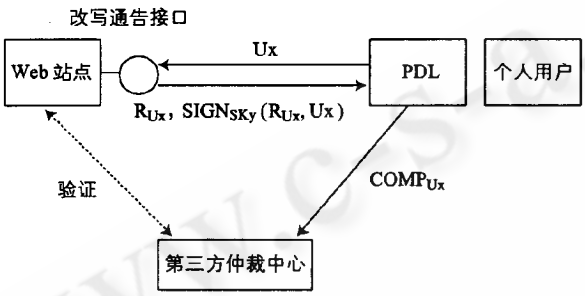

图 2　改写通告

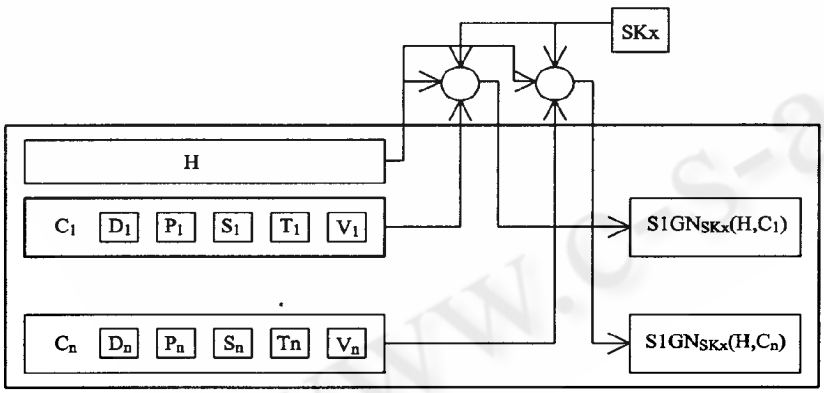

图 3　许可证逻辑视图

4　许可证的设计和实现

许可证的主要组成部分包括:一个报头 H 和一系列的条款 C1,C2,C3,……,Cn。报头 H 包含如下一些信息:许可证的发布者,许可证的获得者,许可证发布的时间,许可证所发布的安全等级等。每一个条款 Ci,描述了许可证发布者所允许的对个人数据集合 Di 所能进行的隐私处理,包括使用目的 Pi,数据共享对象(Si),条款 Ci 的有效期 Ti 等。

条款一般来说是独立设计的,这样主要是为了保证一个条款能够从许可证中被单独提取,而不影响许可证的其余部分,因为有的时候,只需要对许可证中的部分条款进行验证或改写而无需对整个许可证进行处理。被提取的条款通过增加一个合适的报头也可单独作为一个许可证使用。最后,为了验证许可证发布的真实性,确保其中的条款没有被篡改,每个条款 Ci 和许可证报头 H 要被签以许可证发布者的私有密钥 SKx。

图 3 显示了许可证设计和实现的逻辑视图。

5　结束语

本文讨论了 PDL 的设计和实现框架,在此框架下,对用户数据的使用能在用户的授权和监督下进行,和传统的 P3P 规范相比,PDL 不仅能让用户知晓其访问的 Web 站点所提供的隐私策略,而且能监督 Web 站点使用他们数据的方式。

参考文献

1 EPIC, Junkbuster: Pretty poor privacy: A assessment of p3p and internet privacy. http://www.epic.org/reports/prettypoorprivacy.html(2000).

2 Cronar, L., Langheinrich, M., Zurich, E: A P3P Preference Exchange Language 1.0(APPEL1.0). In: W3C Working Draft.(2002) Retrieved 20 Aug. 2002 from http://www.w3c.org/TR/p3p-preferences.html.

3 Benassi, P.: TRUSTe: an online privacy seal program. Communications of the ACM(1999).

4 克劳娜, P3P Web 隐私, 清华大学出版社,2004。