基于信息流的多级安全策略模型研究

王 辉 贾宗璞 申自浩 卢碧波
(河南理工大学计算机科学与技术学院 焦作 454000)

摘 要 内部威胁是企业组织面临的非常严重的安全问题,作为企业最贵重的信息资产——文档,是内部滥用的主要目标。以往的粗粒度安全策略,如最小权限原则、职责分离等,都不足以胜任文档安全化的内部威胁问题。提出了一个崭新的多级安全策略模型,引入了文档信息流和信息流图概念,并提出了相关算法。它能依据系统上下文环境的变化,动态地产生信息流的约束条件,屏蔽可能产生的隐藏信息流通道。

关键词 内部威胁,安全策略,信息流,安全级别,信息流图
中图法分类号 TP393.08 **文献标识码** A

Research of Multi-level Security Policy Model Based on Information Flow

WANG Hui JIA Zong-pu SHEN Zi-hao LU Bi-bo
(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract Insider threat is widely recognized as an utmost important issue for organization security management. As the most important information asset (documents), they are the chief target of insider misuse. The former coarse grained security policies that operate on "the principle of least privilege" or "separate of duty" are not enough to address documents security about insider threat issue. We presented a novel multi-level security policy model and related algorithms, and defined the concept of document information flow and information flow graph. According to system context's change, it will generate dynamic restriction conditions about information flow. And its aim is to prohibit these probable hiding channels of information flow.

Keywords Insider threat, Security policy, Information flow, Security level, Information flow graph

1 引言

如今,随着计算机技术的迅速发展,信息技术深刻地影响着整个社会。几乎所有的企业组织凭借计算机和网络,通过资源共享、信息交换、互操作等方式进行协同工作,如办公自动化系统、工作流管理系统等等。作为企业组织最重要的信息资产——文档,无疑是内部威胁(Insider Threat)的主要目标。在文献[1]中,罗列出了近期美国CSI/FBI官方调查报告的有关数据,从中可知来自内部事件造成的财政损失远远大于外部事件所引起的,因此这些数据应该引起我们的高度重视。

基于策略的管理方式被众多企业组织所接受,以安全策略为中心,构建协同工作环境,通过安全策略检验和约束来保障企业安全化目的的实现。本论文将以文档信息流为研究重点,借鉴了BLP模型[2]、Lattice模型[3]、Chinese Wall模型[4]等的设计理念,克服了以往的粗粒度安全策略模式,提出了一个新颖的文档信息流安全策略模型和信息流有向图模型,达到保障企业上下文环境中文档资源安全化的目的。

2 相关研究

Lattice模型[3]:在模型中,每个资源和用户都分属一个安全级别,分别为:TS,S,C,R,U。Lattice模型适用于信息资源明显分类的系统,是一种安全分级模型。然而,Lattice模型没有考虑到木马等不安全因素的威胁,低级安全用户可能复制和拷贝敏感信息。

BLP模型[2]:该模型是典型的信息保密性多级安全模型,主要用于军事系统,重在保护信息的机密性。BLP模型强调了"下读、上写"规则,用偏序关系可以表示为(s表示主体,o表示客体,SC表示安全级别):1)向下读,当且仅当$SC(s)\geqslant SC(o)$,允许读操作;2)向上写,当且仅当$SC(s)\leqslant SC(o)$,允许写操作。但BLP模型没有采取有效的措施来制约信息的非授权修改,使得非法、越权篡改成为可能。这与维护信息完整性的BIBA模型相反,BLP模型没有考虑完整性和私密性。

Chinese Wall模型[4]:该安全策略最早是由Brewer等人根据现实的商业政策模型提出的。它将公司信息分为3个层次进行存储,底层是单个公司的数据项,中间层是由同一个公司的数据项组合成的公司数据集CD,高层是相互竞争的公司组成的利益冲突类COI,每个公司只能属于一个COI。Brewer-Nash读访问规则,当且仅当s已经读过o或者o属于一个s从未从其中读过任何客体的COI类时,s可以读访问

到稿日期:2009-02-18 返修日期:2009-04-22

王 辉(1975-),男,博士,副教授,主要研究方向为网络安全技术,E-mail:wyhjz@yahoo.com.cn;贾宗璞 男,博士,教授,主要研究方向为网络安全技术;申自浩 男,博士研究生,讲师,主要研究方向为网络安全技术;卢碧波 男,博士,讲师,主要研究方向为网络及图像处理。

o。Brewer-Nash 写访问规则，当且仅当 s 按照 Brewer-Nash 读访问规则可以读 o，且任何与 o 不在同一 CD 集合中的客体都不能够被 s 读访问到时，s 可以写访问 o。尽管 Chinese Wall 模型可以有效预防木马程序的破坏，但是它更多的提供了商业领域安全策略的一种思维方法，考虑到约束条件过于严谨，并没有考虑到多级安全访问的限制条件，因而适用范围有限。

文档控制模型[5]：Suranjan 尝试着对企业文档控制领域进行安全策略模型描述，并对其中的相关实体进行了定义。所提出的文档控制模型在一定程度上，能够抵制内部用户滥用文档事件的发生。然而，它尚存在着明显的缺陷，没有考虑实际企业组织中泄密场景的多样性和文档的安全等级。此外，依据他的安全策略模型设计，因为没有考虑安全级别，比较容易导致“死锁写保护”。即用户 u_0 所打开的文档集，很有可能是其他若干用户权限文档集的并集，这种场景在没有文档安全级时发生的概率是相当高的。结果，用户 u_0 打开的文档集统统不能编辑。

在研究分析上述安全策略模型的基础上，基于文档信息流的设计构想，提出了一个多级安全策略模型。它融合了自主访问控制和强制访问控制两种模式，借鉴了 Lattice 模型、BLP 模型、文档控制模型等的设计思想，在文档安全级别上采用了 Lattice 模型部分思想，提出了类似 BLP 模型的允许“下读”，但禁止“下写”的设计规则，以及采纳了文档控制模型里的信息流概念想法，最终提出了一个新型的基于信息流的多级安全策略模型。

3 文档信息流模型 DIF

定义 1 $DIF=(S,D,A,SC,C,\rightarrow)$，其中

1)文档访问的发起者就是主体，主体集合用 S 表示，其中 $s\in S$，s 表示单个主体。这里，主体既可以是用户，也可以是进程。

2)被动的主体行为承担者就是客体，这里专指文档，文档集合用 D 表示，其中 $d\in D$，d 表示单个文档。

3)主体对文档的操作集合用 A 表示，$A=\{r,w,a,e\}$，这里，重在考虑信息文档，以读(r)、写(w)操作为主。

4)有限集合 SC 定义了所有文档的安全类别，$SC=$｛公开，秘密，机密，绝密｝。

5)有限集合 C 表示约束集合，是施加在文档操作上的一些限制，可以划分为静态约束和动态约束。静态约束是依据已知的威胁，在一定时间内保持不变的约束。动态约束是依据系统环境的变化，动态强制性的约束，以保证文档安全。例如，①文档仅能在工作时间访问，其他时间禁止访问。②在特殊条件得到满足的情况下，禁止对文档编辑操作等。

6)二元关系→表示了两个文档之间的信息流动关系。如果 $d_i\rightarrow d_j$，则表明信息流可以从 d_i 流向 d_j。

泄密场景一

在企业组织中，常见的文档组织结构如图 1 所示。最底层为企业的公共文档集，作为企业职员都有权限去访问该文档集。中间层，分别是各部门的机密文档集，出于商业机密的考虑，各部门之间机密文档集是相互独立的。除非企业授权，否则，有权限访问部门 1 中机密文档的职员，将没有权限访问其他部门的机密文档。最高层，是涉及整个企业组织的最高商业机密——绝密文档集，内容将会覆盖各部门机密文档集中的有关数据和内容。

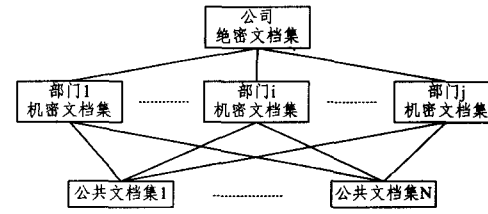

图 1 泄密场景

如果企业只是依据各职员的岗位职能，进行角色授权，没有对文档间信息流的流向进行约束，那么根本达不到对涉密文档的安全性要求。例如，存在这样一个简单场景，普通职员 s_0 仅仅拥有对公开文档的访问权，如公开文档 d_0，可以表示成三元组$(s_0,d_0,r/w)$。职员 s_1 拥有机密文档访问权，可以访问文档 d_0 和 d_1，其中 d_1 是机密文档，三元组表示为$(s_1,d_0,r/w)$和$(s_1,d_1,r/w)$。文档泄密可以通过下列操作序列(Action Sequence)完成。

(1)s_1 打开普通文档 d_0；

(2)s_1 打开机密文档 d_1 进行读操作(如 copy)；

(3)s_1 对文档 d_0 进行写操作(如 plaster)；

(4)s_0 打开文档 d_0 进行读取操作。

结果，s_0 间接地对机密文档 d_1 进行了访问，即在文档 d_0 与 d_1 之间存在隐藏信息流通道，$d_1\rightarrow d_0$。

为了对文档间的信息流进行约束，杜绝出现文档泄密场景 1 中的隐藏通道，本文借鉴了 Lattice 模型和 BLP 模型的设计思想，采用了信息文档的多级安全模型，将 DAC 和 MAC 控制模式相结合，对信息流进行了定义。在允许下读的同时，为了防止低级用户利用潜藏信息流通道窃取敏感信息文档的有关内容，强制性规定了“上写”规则。

定义 2 对于文档安全类别集合 SC，如果信息流 $d_i\rightarrow d_j$ 成立，当且仅当 $SC(d_i)\leqslant SC(d_j)$成立。

定义 2 说明了信息流只能从低级向高级或同级之间流动，即只可上写操作，而不能向下写。依据定义 2，由于文档泄密场景 1 中 $SC(d_0)\leqslant SC(d_1)$，因此信息流通道 $d_1\rightarrow d_0$ 将无法存在，故杜绝了此类泄密场景的发生。

泄密场景二

企业组织在现实中出于最小权限原则和职责分离原则的安全性考虑，会将保密文档信息按照某种范畴或职能进行分类管理。这里，为了便于分析，假设保密文档依据部门职能进行分类管理。但是职员将依据自身角色的不同，而拥有不同的权限，在能够访问公开文档集的同时，或还能访问某部门保密文档的一个子集，或还能访问多个部门保密文档的一个子集。

在定义 2 中，通过强制性的“向上写”规则，杜绝了文档上下密级之间的隐藏信息流通道，但忽略了同级之间隐藏通道的分析。

a)访问文档集相交场景

例如，$D'=$｛部门 1 机密文档集｝，$D''=$｛部门 2 机密文档集｝，$D^*=$｛部门 3 机密文档集｝，并且有 $SC(D')=SC(D'')=SC(D^*)=$｛机密｝。对 $s_1,s_2\in S$ 来说，假定用户 s_1 拥有访问 D'集合中部分文档的权限，即 $D(s_1)=\{d\mid d\in D'\wedge(s_1,d,r/w)\}$，用 D_1 表示。用户 s_2 拥有访问 D'集合和 D''集合中部分

文档的权限，即 $D(s_2)=\{d|d\in D'\cup D''\wedge(s_1,d,r/w)\}$，用 D_2 表示。如图 2 所示，如果 $D_{12}=D_1\cap D_2$ 不为空，则说明存在一个文档集 D_{12}，可以被用户 s_1 和 s_2 同时访问。

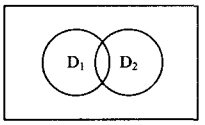

图 2　相交场景

此时，存在这样一个泄密场景。若文档 $d_1\in D_1-D_2$，$d_2\in D_2-D_1$，$d_{12}\in D_1\cap D_2$。文档泄密可以通过下列操作序列完成。

(1)s_1 打开具有写权限的文档 d_1，即(s_1,d_1,w)；

(2)s_2 打开具有读权限的文档 d_2，即(s_2,d_2,r)；

(3)s_2 打开具有写权限文档 d_{12}，即(s_2,d_{12},w)；

(4)s_2 读取文档 d_2 内容(如 copy)。

(5)s_2 对文档 d_{12}进行写操作(如 plaster)；

(6)s_1 打开文档 d_{12}进行读操作(如 copy)；

(7)s_1 对文档 d_1 进行写操作(如 plaster)。

结果，用户 s_1 通过隐藏通道，成功地读取了 d_2 中的机密信息。要注意的是，用户 s_1 对文档 d_2 没有访问权限。在本例子中，存在的信息流通道为 $d_2\rightarrow d_{12}$，$d_{12}\rightarrow d_1$，存在隐藏的信息流通道为 $d_2\rightarrow d_1$。

b)访问文档集不相交场景

假定用户 s_1,s_2,s_3 访问机密文档集分别为 D_1,D_2 和 D_3，并有 $D_1\subseteq D'$，$D_2\subseteq D''$，$D_3\subseteq D'\cup D''\cup D^*$。对于用户 s_1 和 s_2 来说，$D_1\cap D_2=\emptyset$，即用户 s_1 和 s_2 访问文档集不相交，但并不能说明它们之间就一定不存在文档泄密场景。如图 3 所示，如果存在文档集 D_3，有 $D_1\cap D_3\neq\emptyset\wedge D_2\cap D_3\neq\emptyset$，则依然存在隐藏文档泄密通道。

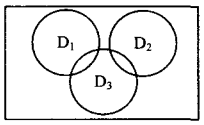

图 3　不相交场景

若 $d_1\in D_1-D_3$，$d_2\in D_2-D_3$，$d_{13}\in D_1\cap D_3$，$d_{23}\in D_2\cap D_3$。如果用户 s_1 希望通过本地文档 d_1，越权读取文档 d_2 中的信息，则存在下列信息流通道：$d_2\rightarrow d_{23}$，$d_{23}\rightarrow d_{13}$，$d_{13}\rightarrow d_1$。其中，隐藏的信息流通道为 $d_2\rightarrow d_1$。相关的操作序列可以参考相交场景中的操作序列，限于篇幅原因这里省略。

从文档泄密场景二中可以看出，仅仅规定了“向上写”强制性规则显然是不够的。为了解决文档相同密级之间信息流隐藏通道问题，很有必要进一步约束文档间的信息流。下面将给出一些相关定义，接着将重点引入一个有向图模型——文档信息流图 G，来解决信息流隐藏通道问题。

定义 3　$\rightarrow$是文档集合 D 上的二元关系，对于 $\forall d_1,d_2\in D$，如果条件$(s,d_1,r)\wedge(s,d_2,w)\wedge SC(d_1)\leqslant SC(d_2)$满足，则有信息流 $d_1\rightarrow d_2$ 成立。

在定义 3 中，表示如果主体 s 能够访问文档 d_1 和 d_2，并且 s 拥有文档 d_2 的写操作权限，则有信息流 $d_1\rightarrow d_2$ 成立。

推论 1　文档集合 D 上的关系$\rightarrow$是可传递的。

对于 $\forall d_1,d_2,d_3\in D$，如果信息流 $d_1\rightarrow d_2$，$d_2\rightarrow d_3$ 存在，则一定有(s,d_1,r)，$(s,d_2,r/w)$，(s,d_3,w)，$SC(d_1)\leqslant SC(d_2)$，$SC(d_2)\leqslant SC(d_3)$成立，从而有(s,d_1,r)，(s,d_3,w)，$SC(d_1)\leqslant SC(d_3)$成立，依据定义，则有信息流 $d_1\rightarrow d_3$ 成立，所以二元关系$\rightarrow$是可传递的。

定义 4(开启文档集，Open-Document，OD)　是指用户在同一时刻打开的文档集合。

4　文档信息流图 G

定义 5　文档信息流图 $G=(V,E)$是一个有限有向图，其中，$V(G)$是一个非空有限集合，表示主体依据自身权限所能访问的文档集，有 $V(G)\subseteq D$；$E(G)$是 $V(G)\times V(G)$的一个子集，表示文档间的信息流$\rightarrow$，见定义 3。如果 $d_1\in V(G)$，$d_2\in V(G)$，并且信息流 $d_1\rightarrow d_2$ 存在，则有$\langle d_1,d_2\rangle\in E(G)$。

对于系统中的任意用户 $s_j\in S$ 而言，依据该用户的角色和读写文档权限，均有一个对应的文档集 D_j 存在，并有可能涉及多个安全级别文档。由定义 5 可知，其对应的文档信息流图 $G(s_j)$将一定存在并唯一，它与用户是一一对应的。

下面是用户 s_j 的文档信息流图$G(s_j)$生成算法。

信息流图生成算法 Generate-Graph

描述：本算法首先生成任一用户 s_j 所对应的访问文档集合 D_j，而后结合用户对集合中的每一文档的读、写权限以及文档的安全级别，依据定义 6，生成该用户对应的信息流图。

输入：企业全体文档集合 D，文档安全类别集合 SC。

输出：s_j 所对应的信息流图$G(s_j)=(V_j,E_j)$。

1)$V_j=\emptyset$；$E_j=\emptyset$；

2)for 所有文档 $d\in D$

2.1)tag(d)=false；//标记初始化

2.2)if (s_j,d,r)为真 then $V_j=V_j\cup\{d\}$；//生成用户 s_j 的访问文档集 D_j 即 V_j

2.3)if (s_j,d,w)为真 then tag(d)=true；//标记文档 d

3)for 所有节点 $v_1\in V_j$

3.1)for 所有节点 $v_2\in V_j$

3.1.1)if tag(v_1) and $SC(v_2)\leqslant SC(v_1)$ then $E_j=E_j\cup\{\langle v_2,v_1\rangle\}$；//将信息流加入到 E_j 中

3.1.2)if tag(v_2) and $SC(v_1)\leqslant SC(v_2)$ then $E_j=E_j\cup\{\langle v_1,v_2\rangle\}$；//将信息流加入到 E_j 中

通过信息流图生成算法，系统可以自动生成企业组织中每一个职员的信息流图。要注意的是，每个具体的信息流图不是一成不变的，它不仅将跟随文档的创建或删除而改变，而且随着文档的密级改变或读写权限的改变而改变。因此，当有文档发生改变时，需要将有关职员的信息流图再次生成，来对应相关改变。

定义 6　活动信息流图(简称 AG)是指某一用户 s 在当前时刻，依据自身的开启文档集 $OD(s)$生成的信息流图。

从定义 6 中不难看出，用户 s 的活动信息流图 $AG(s)$，是依据当前时刻所打开的文档集 OD 对应生成的，生成算法就是信息流图生成算法，只是用开启文档集 OD 替代企业文档集 D，其它不变。它显然是该用户对应信息流图 $G(s)$的一个子图，有 $V(AG(s))\subseteq V(G(s))$，$E(AG(s))\subseteq E(G(s))$。

那么如何利用信息流图解决文档同级之间的隐藏信息流通道呢？简单来说，就是检测当前活动用户 s_0 的开启文档集 $OD(s_0)$，当该用户的活动信息流图 $AG(s_0)$与系统中任意用户 s 的权限信息流图 $G(s)$之间，有向图间存在连通点并且存在连通路径，则表明当前 $OD(s_0)$文档集处于不安全状态，存

在隐藏信息流通道。解决方法就是采用临时强制性约束手段，将连通点对应的可读写文档禁止写操作，截断有向图之间的连通路径，则隐藏信息流通道将不再存在。

例如，对于当前用户 $s_0 \in S$ 来说，假定在时刻 t 时，新打开一个文档 d'，此时他所打开的开启文档集为 $OD(s_0)$，活动信息流图为 $AG(s_0)$。为了判别用户 s_0 的当前文档集 $OD(s_0)$ 是否安全，需要做下列分析。是否存在一个 $s \in S$，其所对应的权限信息流图 $G(s)$ 与有向图 $AG(s_0)$ 之间存在连通点 d'，并且至少存在一条连通路径。假设上述条件均满足，则表明当前活动用户的 $OD(s_0)$ 文档集是不安全的，如图 4 所示，存在隐藏信息流隐藏通道 $\langle d_0, d_1 \rangle$ 和 $\langle d_0, d_2 \rangle$。因而，在活动用户 s_0 新打开文档 d' 的同时，临时强制性约束禁止对文档 d' 的写操作，以截断有向图之间的连通路径，确保隐藏信息流通道不存在。

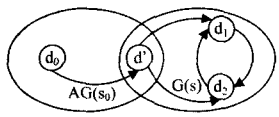

图 4　存在隐藏通道

在图 5 中，发现如果有向图 $AG(s_0)$ 与 $G(s)$ 之间仅仅存在连通点 d'，但是不存在任何连通路径，则表明当前活动用户的 $OD(s_0)$ 文档集是安全的。

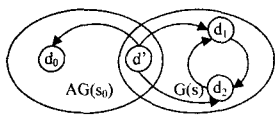

图 5　安全通道

下面给出活动信息流图 $AG(s_0)$ 隐藏信息流通道检测算法。

隐藏通道检测算法 Predict

描述：本算法依据当前活动用户 s_0 新打开的文档 d'，以及对应的活动信息流图 $AG(s_0)$，对全体用户集 S 所对应的信息流图 G 进行遍历，判断是否存在连通点 d' 并且连通路径同时存在。如果存在，遍历终止，并对连通节点文档进行强制性约束，禁止写操作。否则，说明 $OD(s_0)$ 是安全的。

输入：当前用户的活动信息流图 $AG(s_0)$，用户集 S 的各信息流图 G。

输出：$OD(s_0)$ 的动态约束条件。

1) for 所有 s∈S

1.1) if $V(G(s)) \cap \{d'\} \neq \emptyset$ then

1.2.1) for 遍历有向图 $AG(s_0)$ 和 $G(s)$ 中各节点

1.2.1.1) If $\langle d_0, d' \rangle \in E(AG(s_0))$，其中 $d_0 \in V(AG(s_0))$ and $\langle d', d_1 \rangle \in E(G(s))$，其中 $d_1 \in V(G(s))$ and $SC(d_0) \leqslant SC(d_1)$ then //存在隐藏信息流通道

1.2.1.1.1) 临时禁止 (s_0, d', w) 写权限，在关闭后恢复相关权限；//动态约束条件

1.2.1.1.2) 跳出 for 循环，遍历终止；

结束语　由于文档是企业组织信息资产的重要组成部分，为了预防内部威胁，防止内部滥用事件的发生，提出了一个针对文档信息流的多级安全策略模型，来保障企业组织中的信息资产。该模型不仅可以和其他安全策略混合使用，添加相关静态约束规则，而且，它将随着企业操作环境的上下文，对信息流通道进行动态约束，屏蔽相关的隐藏信息流通道，以保障文档操作环境的安全。

但是考虑到内部威胁的复杂性，在未来的研究中，有必要引入已知的各种内部威胁模式，作为该多级安全策略的一种强有力的补充，进行进一步的修订和完善。

参 考 文 献

[1] 王辉，刘淑芬. 一种可扩展的 Insider Threat 预测模型[J]. 计算机学报，2006，29：1346-1355

[2] Bell K，LaPadula L J. Secure computer systems：Unified exposition and multics interpretation[R]. MTR22997. MITRE Corporation，1976

[3] Denning D. A Lattice Model of Secure Information Flow [J]. Communications of the ACM，1976，19：236-243

[4] Brewer D，Nash M. The Chinese Wall security policy[C]//Proceedings of the IEEE Symposium on Research in Security and Privacy. Los Alamitos，CA：IEEE Computer Society Press，1989：206-214

[5] Pramanik S，Sankaranarayanan V，Upadhyaya S. Security Policies to Mitigate Insider Threat in the Document Control Domain [C]//Proceedings of the 20th Annual Computer Security Applications Conference. 2004

(上接第 50 页)

[4] Abadi M. Reconciling two views of cryptography[J]. Journal of Cryptology，2002，5(2)：103-227

[5] Mao Wenbo. Modern Cryptography：Theory and Practice[M]. Prentice-Hall，PTR，2004

[6] Bellare M. Random Oracles are Practical：a Paradigm for designing efficient protocols[C]//First ACM Conference on Computer and Communications Security. New York：ACM Press，1993：62-73

[7] Beaver D. Foundations of secure interactive computing [C]// Joan Feigenbaum：Advances in Cryptology-Crypto'91. Lecture Notes in Computer Science. Berlin：Springer-Verlag，1991：377-391

[8] Yao C. Protocols for secure computations (extended abstract) [C]//23rd Annual Symposium on Foundations of Computer Science. 160-164

[9] Canetti R. Analysis of key exchange protocols and their use for building secure channels[C]//Eurocrypt'01. 2001

[10] Canetti R. Security Analysis of IKE's Signature-based Key Exchange Protocol[C]//Advances in Cryptology- Crypto 2002

[11] Bellare M，Canetti R，Krawczyk H. A Modular Approach to the Design and Analysis of Authentication and Key-exchange Protocols[C]//Proc. of the 30th Annual Symp. on the Theory of Computing. New York：ACM Press，1998：419-428

[12] Goldwasser S，Micali S，Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks[J]. SIAM Journal on Computing，1998，17(2)：281-308

[13] 3GPP. TS 22.934 Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) interworking (Release 6)[S]. Valbonne：3GPP TSG SA，2003

[14] 3GPP. TS 33.234 Wireless Local Network(WLAN) Interworking Security[S]. Valbonne：3GPP，2005