一种基于通信信道容量的多级安全模型

刘 雄,卓雪君,汤永利,戴一奇
(清华大学计算机科学与技术系,北京 100084)

摘 要: 安全模型有多种代表模型,如 BLP 模型和不可推断模型等.这些模型在理论描述或者实际应用方面存在一定的局限性,如 BLP 模型未能考虑隐蔽通道,不可推断模型不适应非确定系统.针对这些模型的不足,本文在 BLP 模型基础上,考虑了隐蔽通道的特性,提出了泄密通道有限容忍的通信信道模型,该模型能通过调节泄密通道信道容量上限来平衡实际系统可用性和安全性.

关键词: 安全模型; BLP 模型; 隐蔽通道; 通信信道模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 10-2460-05

A Multilevel Security Model Based on Communication Channel Capacity

LIU Xiong, ZHUO Xue-jun, TANG Yong-li, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: Many typical security models have been proposed, such as the BLP model and the nondeducibility model, however, these models have some disadvantages and limitations in theoretical analysis or implementation respectively. For instance, BLP model did not take the covert channel into account, and the nondeducibility model cannot be applied to the nondeterministic systems. Considering these shortages brought about by the existing works, this paper take the properties of the covert channel as a main consideration, and propose a novel finite-information-leakage-tolerance communication channel model based on the BLP model. The proposed model finds a tradeoff between the availability and security of the practical system by adjusting the upper bound of the channel capacity of the information leakage.

Key words: security model; BLP model; covert channel; communication channel model

1 引言

在安全模型的发展历史上,出现过多种经典模型,如 BLP 安全模型(Bell-Lapadula Model)[1]、不干扰模型(Noninterference Model)[2]、信息流格模型(Information Flow Lattice Model)[3]和不可推断模型(Nondeducibility Model)[4]等.其中 BLP 模型还衍生出多种改进 BLP 模型,如 CBLP 模型[5]和 L-BLP 模型[6]等.随着安全理论的不断发展,这些模型也不断暴露出自身的局限性,如隐蔽通道[7]的存在,导致 BLP 及其改进模型很难保证系统的安全性;信息流格模型没能考虑隐蔽通道很难消除特性;不干扰模型禁止高等级实体到低等级实体的无规则干扰,规则限制太强,实际系统很难实现;不可推断模型只适应确定系统,对于非确定系统会存在泄密通道[8].

从实际应用来说,绝对安全的信息系统是不存在的,为了保证系统的可用性,某些隐蔽通道的存在是不可避免的,如网络中低安全等级主机向高安全等级主机发送消息时,高安全等级主机需要向低安全等级主机回送 ACK 网络数据包,这会带来高安全等级主机到低安全等级主机的隐蔽通道.而隐蔽通道的存在会降低系统的安全性,因此需要在安全性和可用性之间寻找一个平衡点,使系统既能够保持一定的可用性,又能保证安全性,而目前的多级安全模型,都不能对实际系统的该需求进行描述.

理论研究表明,信息安全的解释应该以香农的信息论作为基础,信息安全应该以控制系统中实体间信息传输为目标[8].系统中实体间隐蔽通道虽然信道容量一般较小,但是同样能泄漏信息.美国国防部发布的橘皮书 TCSEC[9]就要求对 B2 级以上的高等级安全操作系统进行评估时,必须分析隐蔽通道,并指出系统可接受信道容量小于 1bit/s 的隐蔽通道.有关隐蔽通信信道容量计算有很多研究成果[10~13],本文不关注隐蔽通道信道容量的计算方法,而是在隐蔽通道信道容量能够计算的前提条件下,在 BLP 模型基础上,结合通信信息论,提出了一种通信信道模型,对多级安全进行有限安全描述,给出系统在泄密通道容忍范围之内的模型表述.

收稿日期:2009-06-20;修回日期:2009-10-27

2　多级安全模型通信信道表示

2.1　状态变量和系统的定义

本节将给出在所提出模型描述中使用的主要的状态变量.

2.1.1　基本元素

(1)实体集合 S.表示系统中实体集合,S 中元素如 S_i, S_j 等代表系统中实体.

(2)等级集合 C,类别集合 K,敏感标记集合 $L = C \times K$.表示实体安全等级.等级用数字表示,数字越大等级越高;类别用集合表示,表示可访问实体范围.

(3)定义 L 上的二元关系 $\geqslant$.如果有 $L_i, L_j \in L$, $C_i, C_j \in C$, $K_i, K_j \in K$, $L_i = (C_i, K_i)$, $L_j = (C_j, K_j)$,则 $L_i \geqslant L_j :=(C_j \leqslant C_i) \wedge (K_i \supseteq K_j)$,其中 $L_i \geqslant L_j$ 表示 L_i 支配 L_j.约定系统最低安全等级为 $L_{\min}$.

(4)请求集合 R,判定集合 D. $R = S \times S \times \{send, get, sag\}$, $D = \{yes, no, error\}$, *send* 表示发送信息,*get* 表示获取信息,*sag* 表示既发送信息又获取信息,如 $(S_i, S_j, send)$表示 S_i 向 S_j 发送信息的请求;*yes* 表示请求通过,*no* 表示请求否决,*error* 表示不能判定.

(5)信道集合 $E = \{e(S \times S)\}$, $e(S_i, S_j)$表示从实体 S_i 到实体 S_j 的信道容量. $e(S_i, S_j) = dc(S_i, S_j) + cc(S_i, S_j)$,其中,$dc(S_i, S_j)$ 表示从实体 S_i 到实体 S_j 的实际直接信道容量,$cc(S_i, S_j)$ 表示从实体 S_i 到实体 S_j 的隐蔽信道容量.

(6)自主安全信息流矩阵 $\boldsymbol{M}$.矩阵 $\boldsymbol{M}$ 中元素 $M_{ij} = 1$ 表示自主安全特性允许信息流从实体 S_i 至实体 S_j, $M_{ij} = 0$ 表示禁止.

(7) $F = \{(f_s, f_c) \mid \forall S_i \in S, f_s(S_i) \geqslant f_c(S_i)\}$ 为安全等级标记函数集合,f_s 是实体最大安全等级标记函数,f_c 是实体当前安全等级标记函数.如果 S_i 为系统输入,那么其 f_c 和 f_s 等同.

(8)系统信息流矩阵 $\boldsymbol{B}$. $\boldsymbol{B}_{ij} = 1$ 表示系统允许从 S_i 至 S_j 信息流, $B_{ij} = 0$ 表示禁止从 S_i 至 S_j 信息流.

(9)系统状态集合 $U = E \times \boldsymbol{M} \times F \times \boldsymbol{B}$.

2.1.2　安全特性

系统状态 u 是 ε 上限安全状态 *iff* 状态 u 满足以下三个安全特性.

(1)信息流安全特性

状态 $u = (E, \boldsymbol{M}, f, \boldsymbol{B})$满足: $\forall (S_i, S_j), B_{ij} = 1, \Rightarrow f_c(S_j) \geqslant f_c(S_i)$.

(2)自主安全特性(ds-特性)

状态 $u = (E, \boldsymbol{M}, f, \boldsymbol{B})$满足: $B_{ij} = 1 \Rightarrow M_{ij} = 1$.

(3)通道特性

状态 $u = (E, \boldsymbol{M}, f, \boldsymbol{B})$满足: $\forall (S_i, S_j), e(S_i, S_j) > \varepsilon, \Rightarrow f_c(S_j) \geqslant f_c(S_i)$.

2.1.3　状态转换规则

状态转换规则定义为 $\rho: R \times U \rightarrow D \times U$.

对 $R_k \in R, D_m \in D$,规则 $\rho(R_k, u) = (D_m, u^*)$保持 ε 上限安全状态 *iff* 状态 u 与 u^* 是 ε 上限安全状态.

2.1.4　基本安全公理

如果系统的初始状态是 ε 上限安全的,并且所有的转换规则是 ε 上限安全的,那么该系统是 ε 上限安全的.

2.2　信道容量及判定执行

实体间的通信信道分为两类:直接通道和隐蔽通道.直接通道是系统设计用来实现实体间通信的,因此系统可以控制其通断,而且其信道容量比较大,一般远远大于本文中的 ε 上限安全中的 ε.隐蔽通道本不是设计用来进行通信的,但是实际上却可以达到通信的目的.正因为该通道不是设计者的设计意图,所以通信容量较小,且系统很难控制其通断.在本文中,默认直接通信信道容量远大于 ε,系统可以控制其通断,但是系统不能控制隐蔽通道的通断.

系统根据信息流矩阵 $\boldsymbol{B}$ 来控制直接通信信道的通断.令 $dd(S_i, S_j)$ 表示系统设计从实体 S_i 到实体 S_j 的最大直接信道容量,系统需要达到的控制效果如下:

$$\forall (S_i, S_j), B_{ij} = 0, \Rightarrow dc(S_i, S_j) = 0;$$

$$\forall (S_i, S_j), B_{ij} = 1, \Rightarrow dc(S_i, S_j) = dd(S_i, S_j).$$

即在 $B_{ij} = 0$ 时,关闭 S_i 到 S_j 直接通信信道,在 $B_{ij} = 1$ 时,开通 S_i 到 S_j 直接通信信道.

2.3　状态初始化及状态迁移

首先给出几个相关定义.

定义 1　定义运算符 $\oplus$ 为安全级上的最小上界运算符,运算符 $\oplus$ 具有如下性质:

(1)设实体 S_i,和 S_j,它们的当前安全等级分别为 L_i, L_j,设: $L_i = (C_i, K_i)$, $L_j = (C_j, K_j)$,定义 $\max(C_i, C_j) = (C_j \leqslant C_i)?\ C_i : C_j$,则 $S_i \oplus S_j = L_i \oplus L_j = (C_i, K_i) \oplus (C_j, K_j) = (\max(C_i, C_j), K_i \cup K_j)$.

(2) $\oplus\{S_1, S_2, \cdots S_n\} = S_1 \oplus S_2 \oplus, \cdots \oplus S_n$.

定义 2　定义系统 W 对应的有向图为 $D_w(V, A)$, V 表示顶点集,A 表示弧集.图 $D_w(V, A)$构建方法为:对于 W 中每一个实体 S_i,在图中构建一个标号为 S_i 的顶点;对于 W 中任意两个实体 S_i 和 S_j,如果 $e(S_i, S_j) > \varepsilon$,则图中添加一条弧 $a(S_i, S_j)$.

说明:在本文中,S_i 或 S_j 表示形式可能指系统或者模型中实体,也可能表示有向图中的某一个节点,具体所指根据上下文关系所确定.

定义 3　图 $D_w(V, A)$中,所有从顶点 S_i 可达的顶点集合称为 S_i 的可达顶点集,记为 $\mathrm{Reach}(S_i)$.

定义 4 定义节点的可达节点集安全等级更新操作为 Update(S_i)函数,其所进行操作为:For every S_k in Reach(S_i),$f_c^*(S_k) := f_c(S_k) \oplus f_c(S_i)$.

模型状态初始化和状态迁移规则描述如下.

(1)状态初始化

初始化过程如下:

(ⅰ)for B 中每一元素 $B_{ij}, B_{ij} := 0$;

(ⅱ)对于 S 中每一个元素 S_i 作如下处理:

(a)系统管理员指定 $f_s(S_i)$;

(b)$f_c(S_i) := L_{\min}$;

(ⅲ)构建系统 W 对应的有向图 $D_w(V, A)$;

(ⅳ)对于 S 中每一个元素 S_i 作如下处理:

(a)if S_i 为系统输入,then: $f_c(S_i) := f_s(S_i)$;

(b)if (for every S_k in Reach(S_i), $f_s(S_k) \geqslant f_c(S_i)$) then: Update($S_i$),else:系统初始化失败.

(2)状态迁移

系统接收到的请求有三种,分别为 $r(S_i, S_j, send)$、$r(S_i, S_j, get)$和 $r(S_i, S_j, sag)$,对它们的处理规则分别如下:

在状态 $u = (E, M, f, B)$下,对于请求 $r(S_i, S_j, send)$

if ($M_{ij} = 1$) and (for every $S_k \in \text{Reach}(S_j) \cup \{S_j\}$, $f_s(S_k) \geqslant f_c(S_i)$) ,then:

(a)$f_c^*(S_j) := f_c(S_j) \oplus f_c(S_i)$;Update($S_j$);

(b)授权 $r(S_i, S_j, send)$(即 $d := yes, B_{ij}^* := 1$);

(c)有向图 $D_w(V, A)$添加弧(S_i, S_j).

else: 拒绝请求.

在状态 $u = (E, M, f, B)$下,对于请求 $r(S_i, S_j, get)$

if ($M_{ji} = 1$) and (for every $S_k \in \text{Reach}(S_i) \cup \{S_i\}$, $f_s(S_k) \geqslant f_c(S_j)$), then:

(a)$f_c^*(S_i) := f_c(S_j) \oplus f_c(S_i)$;Update($S_i$);

(b)授权 $r(S_i, S_j, get)$(即 $d := yes, B_{ji}^* := 1$);

(c)有向图 $D_w(V, A)$添加弧(S_j, S_i).

else:拒绝请求.

在状态 $u = (E, M, f, B)$下,对于请求 $r(S_i, S_j, sag)$

if ($M_{ij} = 1$) and ($M_{ji} = 1$) and (for every S_k (Reach(S_j) $\cup \{S_j\}$, $f_s(S_k) \geqslant f_c(S_i)$) and (for every $S_k \in \text{Reach}(S_i) \cup \{S_i\}$, $f_s(S_k) \geqslant f_c(S_j)$)

then:

(a)$f_c^*(S_j) := f_c(S_j) \oplus f_c(S_i)$;Update($S_j$);

(b)$f_c^*(S_i) := f_c(S_j) \oplus f_c(S_i)$;Update($S_i$);

(c)授权 $r(S_i, S_j, sag)$(即 $d := yes, B_{ij}^* := 1, B_{ji}^* := 1$);

(d)有向图 $D_w(V, A)$添加弧(S_i, S_j)和(S_j, S_i);

else:拒绝请求.

3 安全性分析

可以证明满足通信信道模型状态初始化及状态迁移规则的系统是 ε 上限安全的.首先给出一个相关定理.

定理 1 系统在 $u(E, \boldsymbol{M}, f, \boldsymbol{B})$状态满足 $\forall S_i \in S$, $\forall S_k \in \text{Reach}(S_i)$, $f_c(S_k) \geqslant f_c(S_i)$,那么 $\forall S_j \in S$,系统在执行:

操作(1) 更改 $f_c(S_j)$的值为 $f_c^*(S_j)$且 $f_c^*(S_j) \geqslant f_c(S_j)$;

操作(2) Update(S_j)后,系统状态 $u^*(E^*, M^*, f^*, B^*)$满足 $\forall S_i \in S$, $\forall S_k \in \text{Reach}(S_i)$, $f_c^*(S_k) \geqslant f_c^*(S_i)$.

证明:对于 $\forall S_i \in S$, $\forall S_k \in \text{Reach}(S_i)$,考虑节点 S_k、S_i 和集合 Reach(S_j)之间的从属关系,一共有以下几种可能情况:

情况(a) $S_i \in \text{Reach}(S_j) \cup \{S_j\}$, $S_k \in \text{Reach}(S_j) \cup \{S_j\}$;

情况(b) $S_i \notin \text{Reach}(S_j) \cup \{S_j\}$, $S_k \in \text{Reach}(S_j) \cup \{S_j\}$;

情况(c) $S_i \in \text{Reach}(S_j) \cup \{S_j\}$, $S_k \notin \text{Reach}(S_j) \cup \{S_j\}$;

情况(d) $S_i \notin \text{Reach}(S_j) \cup \{S_j\}$, $S_k \notin \text{Reach}(S_j) \cup \{S_j\}$;

情况(a),由于有 $S_k \in \text{Reach}(S_i)$,所以有 $f_c(S_k) \geqslant f_c(S_i)$.执行完操作(1)、(2)后,$f_c^*(S_i) = f_c(S_i) \oplus f_c^*(S_j)$,$f_c^*(S_k) = f_c(S_k) \oplus f_c^*(S_j)$,显然满足 $f_c^*(S_k) \geqslant f_c^*(S_i)$.

情况(b),由于有 $S_k \in \text{Reach}(S_i)$,所以有 $f_c(S_k) \geqslant f_c(S_i)$.执行完操作(1)、(2)后,$f_c^*(S_i) = f_c(S_i)$,$f_c^*(S_k) = f_c(S_k) \oplus f_c^*(S_j)$,显然满足 $f_c^*(S_k) \geqslant f_c^*(S_i)$.

情况(c),与定义 2 矛盾,这种情况不可能出现.

情况(d),由于有 $S_k \in \text{Reach}(S_i)$,所以有 $f_c(S_k) \geqslant f_c(S_i)$.执行完操作(1)、(2)后,$f_c^*(S_i) = f_c(S_i)$,$f_c^*(S_k) = f_c(S_k)$,显然满足 $f_c^*(S_k) \geqslant f_c^*(S_i)$.

综合上述,定理 1 得证.

根据分析,可以得出如下结论.

定理 2 系统状态成功初始化后的系统状态是 ε 上限安全的.

证明:设初始化过程的步骤完成之后状态为 u^*,此状态下信息流矩阵 B 所有元素都等于 0,所以 u^* 显然满足信息流安全特性和自主安全特性.设初始化过程的步骤(1)~(3)完成之后状态为 u,由步骤(2)可知 u 状态下对于任何实体 S_i,都有 $f_c(S_i) := L_{\min}$,显然状态 u 满足 $\forall S_i \in S$, $\forall S_k \in \text{Reach}(S_i)$, $f_c(S_k) \geqslant f_c(S_i)$,随后的步骤(4)符合定理 1 描述情况,则根据定理 1,u^* 满足 $\forall S_i \in S$, $\forall S_k \in \text{Reach}(S_i)$, $f_c^*(S_k) \geqslant f_c^*(S_i)$,易证 u^* 满足信息流安全特性和通道特性.综合上述 u^* 满足

模型的三个安全特性.故系统状态初始化过程成功后,系统状态是 ε 上限安全的.

定理 3　状态迁移规则是 ε 上限安全的

证明:首先证明对于请求 $r(S_i, S_j, send)$的处理规则是 ε 上限安全的.设状态 u 是初始状态,且是 ε 上限安全的,状态 u^* 是规则执行完时的状态.对于请求 $r(S_i, S_j, send)$,规则检验了请求是否符合自主安全特性,保证了状态 u^* 满足自主安全特性.规则的操作符合定理 1 描述的情况,因此状态 u^* 满足 $\forall S_i \in S, \forall S_k \in \mathrm{Reach}(S_i), f_c^*(S_k) \geqslant f_c^*(S_i)$.易证 u^* 满足信息流安全特性且满足通道特性.综合上述,u^* 满足模型的三个安全特性.故对于请求 $r(S_i, S_j, send)$的处理规则是 ε 上限安全的.

同理可证明对于请求 $r(S_i, S_j, get)$的处理规则是 ε 上限安全的.

对于请求 $r(S_i, S_j, sag)$的处理规则实际上是将 $r(S_i, S_j, send)$和 $r(S_i, S_j, get)$的处理规则合二为一的结果,因此同理可以得到证明.综合上述定理 3 得证.

定理 4　满足通信信道模型状态初始化及状态迁移规则的系统是 ε 上限安全的

证明:由定理 2 和定理 3 及基本安全公理,该系统是 ε 上限安全的.

4　应用举例

下面举一个例子来说明模型的应用.设系统有实体 S_1, S_2, S_3, S_4 和 S_5,其中 S_1 为系统高级输入,S_2 为系统低级输入,S_3 和 S_4 为系统高级输出,S_5 为低级输出.它们的最大安全等级以及它们之间的隐蔽通道最大信道容量如表 1 所示.

表 1　隐蔽通道容量及最大安全等级表(信道容量单位:bit/s)

S_i	S_1	S_2	S_3	S_4	S_5
$cc(S_1, S_i)$		0	20	10	10
$cc(S_2, S_i)$	0		10	20	20
$cc(S_3, S_i)$	20	10		10	10
$cc(S_4, S_i)$	20	20	20		30
$cc(S_5, S_i)$	20	20	30	10	
$f_S(S_i)$	(c,h)	(c,l)	(c,h)	(c,h)	(c,l)

其中:$(c,h) \geqslant (c,l) \geqslant L_{\min}$

表 2　系统初始化状态表

ε(bit/s)	$f_c(S_1)$	$f_c(S_2)$	$f_c(S_3)$	$f_c(S_4)$	$f_c(S_5)$
5	(c,h)	*error*	*error*	*error*	*error*
15	(c,h)	(c,l)	(c,h)	(c,l)	(c,l)
25	(c,h)	(c,l)	$L_{\min}$	$L_{\min}$	$L_{\min}$
35	(c,h)	(c,l)	$L_{\min}$	$L_{\min}$	$L_{\min}$

设有请求序列 $r(S_3, S_1, get)$、$r(S_4, S_1, get)$、$r(S_3, S_2, get)$以及 $r(S_4, S_3, get)$.系统初始化状态如表 2 所示,系统对请求序列判决情况如表 3 所示.如果表项中有 *error*,表示系统不能满足安全性.

表 3　系统判决情况表

ε(bit/s)	$r(S_3, S_1, get)$	$r(S_4, S_1, get)$	$r(S_3, S_2, get)$	$r(S_4, S_3, get)$
5	*error*	*error*	*error*	*error*
15	*yes*	*no*	*yes*	*no*
25	*yes*	*no*	*yes*	*no*
35	*yes*	*yes*	*yes*	*yes*

由表中数据可以看出,当 ε = 5bit/s 时,系统初始化不能满足模型安全特性,系统无法运行;当 ε = 15bit/s 和当 ε = 25bit/s 时,系统虽然可以运行,但是损失了部分可用性,如 S_4 的最大安全等级足够大,但是系统拒绝执行 $r(S_4, S_1, get)$,因为一旦允许执行就会违反模型通道安全特性;当 ε = 35bit/s 时,ε 值大于所有隐蔽通道信道容量,此时系统可用性较好,所有请求都顺利执行.

从以上结果来看,用户可以根据安全性和可用性具体需求,选取不同的 ε 值.ε 取值越小,系统越安全,但可用性较差;反之系统安全性差,但可用性较好.当 ε 取极小值 0 时,系统可以保证绝对安全.

5　结束语

本文提出的通信信道模型考虑了隐蔽通道及其难以消除特性,提出了泄密通道信道容量有限容忍的安全模型,用户可以根据实际系统的具体需求,设置不同的泄密通道容量上限来调节系统的可用性和安全性.和 BLP 模型相比,该模型考虑了隐蔽通道的存在,安全性得到加强;和信息流格模型相比,该模型考虑了隐蔽通道不可消除特性;和不干扰模型相比,该模型可以适度放松规则限制强度,可用性增强;和不可推断模型相比,该模型可以量化控制泄密通道.

模型实现的前提是能够有效计算系统中实体间隐蔽通道信道容量,这部分工作目前已经有很多研究成果,但是仍然是研究的一个热点和难点,需要有更深入的研究.

参考文献:

[1] Bell D E, LaPadula L J. Secure computer system: Unified exposition and MULTICS interpretation [R]. Bedford, MA: The MITRE Corporation, 1976.

[2] Goguen J, Meseguer J. Security policies and security models [A]. Proceedings of IEEE Symposium on Security and Privacy, 1982 [C]. Los Alamitos: IEEE Computer Society Press, 1982.11 – 20.

[3] Denning D E. A lattice model of secure information flow [J]. Communication of the ACM, 1976, 19(5): 236 – 243.

[4] Sutherland D, A model of information[A]. Proc of the 9th National Computer Security Conference[C]. Gaithersburg, MD: National Bureau of Standards, National Computer Security Center, 1986. 175 – 183.

[5] 谭智勇,刘铎,司天歌,等.一种具有可信度特征的多级安全模型[J].电子学报,2008,36(8):1637 – 1641.
Tan Zhi-yong, Liu Duo, Si Tian-ge, et al. A multilevel security model with credibility characteristics[J]. Acta Electronica Sinica, 2008, 36(8): 1637 – 1641. (in Chinese)

[6] 司天歌,张尧学,戴一奇.局域网络中的 L-BLP 安全模型[J].电子学报,2007,35(5):1005 – 1008.
Si Tian-ge, Zhang Yao-xue, Dai Yi-qi. L-BLP security model in local area network[J]. Acta Electronica Sinica, 2007, 35(5): 1005 – 1008. (in Chinese)

[7] Lampson, Butler W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613 – 615.

[8] J Todd Wittbold, Dale M Johnson. Information flow in nondeterministic systems[A]. In Proceedings of the 1990 IEEE Computer Society Symposium on Computer Security and Privacy[C]. Oakland, CA: IEEE, 1990. 144 – 161.

[9] DoD 5200.28-STD, Trusted computer system evaluation criteria[S].

[10] Gray, James W III. Toward a mathematical foundation for information flow security[A]. Proceedings of the Symposium on Security and Privacy[C]. Oakland, CA: IEEE Computer Society, 1991. 21 – 34.

[11] Jonathan K Millen. Covert channel capacity[A]. Proceedings of the 1987 IEEE Computer Society Symposium on Computer Security and Privacy[C]. Oakland, CA: IEEE Computer Society, 1987. 60 – 66.

[12] V Berk, A Giani, G Cybenko, Detection of covert channel encoding in network packet delays[R]. Dartmouth: Department of Computer Science, Dartmouth College, 2005.

[13] Chen Li, Ju Shiguang, Zhou Conghua, et al. Covert channel capacity analysis based on entropy[A]. International Symposium on Information Science and Engineering, ISISE'08[C]. Shanghai, China: IEEE, 2008. 363 – 367.

作者简介:



刘 雄 男,1978 年 10 月生于湖南耒阳.清华大学计算机科学与技术系在读博士生,从事网络与信息系统安全方面的研究工作.
E-mail: liuxiong@gmail.com

卓雪君 女,1984 年 12 月出生于上海.清华大学计算机科学与技术系在读博士生,从事网络与信息系统安全方面的研究工作.
E-mail: zhuoxj07@mails.tsinghua.edu.cn

汤永利 男,1972 年生于河南孟州,清华大学计算机科学与技术系在站博士后,研究方向包括网络与信息安全风险研究、多级系统安全等. E-mail: tangzili@163.com

戴一奇 男,1946 年生于浙江,清华大学计算机科学与技术系教授,博士生导师,主要研究方向为网络信息安全.
E-mail: dyq@theory.cs.tsinghua.edu.cn

(上接 2459 页)

[7] 蒲保兴,杨路明,王伟平.网络拓扑未知环境下确定性网络编码数据传输[J].电子学报,2009,37(10):2119 – 2124.
Pu Bao-xing, Yang Lu-ming-, Wang Wei-ping. A deterministic data transmission approach with network coding under unknown network topology[J]. The Acta Electronica Sinica, 2009, 37(10): 2119 – 2124. (in Chinese)

[8] Min, Yang, Yuanyuan, Yang. A linear inter-session network coding scheme for multicast[A]. Proceedings of the 2008 Seventh IEEE International Symposium on Network Computing and Applications[C]. Washington, DC, USA: IEEE Computer Society, 2008. 177 – 184.

[9] Zhijian Qu, Yuefeng Ji, Lin Bai, et al. Key module for a novel all-optical network coding scheme[J]. Chinese Optics Letters, 2010, 8(8): 753 – 756.

[10] Kaikai Chi, Xiaohong Jiang, HoriguchiS, et al. Topology design of network-coding-based multicast networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(5): 627 – 640.