第38卷 第21期 计 算 机 工 程 2012年11月
Vol.38 No.21 Computer Engineering November 2012

·安全技术· 文章编号：1000—3428(2012)21—0141—04 文献标识码：A 中图分类号：TP393.08

一种面向局域网的多级安全模型

王 浩，陈泽茂，谌双双

(海军工程大学电子工程学院，武汉 430033)

摘 要：为保证局域网环境下共享信息的机密性，提出一种基于BLP模型的局域网多级安全模型MLS-LAN。引入密级标定部件，标定动态信息资源的安全级别，利用接入认证部件和访问控制部件，定义接入认证、信息共享和通信关系控制等规则，由此实现多级信息资源的安全共享。理论分析结果表明，该模型可以对信息共享实施可靠的访问控制，提高了局域网信息共享的安全性。

关键词：多级安全模型；信息共享；访问控制；BLP模型；网络安全；信息密级标定

A Multi-level Security Model for Local Area Network

WANG Hao, CHEN Ze-mao, CHEN Shuang-shuang

(College of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China)

【Abstract】 In order to ensure the confidentiality of information sharing in Local Area Network(LAN), a multi-level security model for LAN based on BLP model named MLS-LAN is proposed. It estimates the security-level of dynamic information resources by introducing security-level calibration facility in LAN, and it uses access authentication facility and access control facility to define access authentication, information sharing and communication relationship control rules, so that secure sharing for multi-level information in LAN is realized. Theoretical results show the model can provide reliable access control to information sharing and enhance its security.

【Key words】 multi-level security model; information sharing; access control; BLP model; network security; information security-level calibration

DOI: 10.3969/j.issn.1000-3428.2012.21.038

1 概述

多级安全信息系统[1]是指一类包含各种敏感等级的信息、在不危及信息安全的情况下能同时为不同安全等级用户提供访问服务的系统。进入后PC时代，由于计算机网络的飞速发展以及构建成本的降低，政府和企业为优化工作环境和提高工作效率，纷纷采用网络化办公。目前，在政府和大型企业的各类信息网络中普遍存在以下现象：(1)不同安全等级的信息共存于同一个网络中；(2)不同安全等级的人员和进程可访问同一个网络；(3)需要集中不同安全等级的人员、进程和数据协同完成一项任务。此类信息网络具有明确的多级安全需求，特别是政府、军队、银行等对信息安全较为敏感的部门，对局域网的多级安全需求尤为迫切。因此，国内外在多级安全模型和多级安全系统部署架构上开展了深入研究。

CORBA(Common Object Request Broker Architecture)是美国海军研究实验室开发的多级安全网络部署方案，它采用对象代理处理来自服务器和客户端的请求数据[2]。由于CORBA安全架构主要面向商业，采用的是“胖服务器瘦客户端”模式，其安全性、通用性和可靠性都有局限。从20世纪90年代末至今，美国海军研究生院信息安全研究与探索中心一直致力于MYSEA(Monetery Security Architecture)[3]多级安全网络方案的研究工作。MYSEA系统运行在多重的安全等级上，依靠一些小的具有高可信度的设备构建多级安全环境。但MYSEA并非一个真正的分布式架构，不能实现所有网络的互联，并由于服务器负载过重而存在功能上的瓶颈。

在国内，文献[4]提出一种引入了动态监控设备和资源服务器的L-BLP模型，主要用于解决多级信息系统中静态资源的信息安全共享问题，而对于网络数据包等动态资源只能实施主机层面的访问控制。文献[5]提出的分布式多级安全网络部署方案将网络按主机密级的不同划分为多个子网，并设置专用的多级服务器来处理不同子网间的访问。实际上，此部署架构是以不同密级的子网作为主体，无法对主机进行保护，而且它要求相同安全级别的主机处于独立的子网中，限制了网络的物理分布。

本文基于BLP模型[6-7]，通过引入接入认证部件、密级标定部件和访问控制部件，提出一种新的局域网多级安全模型MLS-LAN，该模型通过提供网络接入认证、标定共享数据的安全级别，对网络节点间的通信关系进行约束，实施可靠的访问控制，实现网络环境中的信息共享控

基金项目：中国博士后科学基金资助特别项目(201003757)

作者简介：王 浩(1988－)，男，硕士研究生，主研方向：网络安全；陈泽茂，副教授、博士；谌双双，硕士

收稿日期：2012-01-05 **修回日期**：2012-02-29 **E-mail**：wanghao821@yahoo.cn

制，以保护局域网环境下信息的机密性。

2 MLS-LAN 安全模型

2.1 模型元素

MLS-LAN 安全模型中的相关约定和主要元素的定义如下：

约定 1 e 表示接入认证部件，是 MLS-LAN 中为网络接入提供认证的部件。

约定 2 q 表示密级标定部件，是 MLS-LAN 中对信息客体进行密级标定的部件。

约定 3 g 表示访问控制部件，是 MLS-LAN 中为主体间信息共享提供访问控制的部件。

定义 1 主体集合 S

$S=\{s_1,s_2,\cdots,s_i\}$，表示对实体主动施加操作的实体集合，如用户和进程。

定义 2 客体集合 O

$O=\{o_1,o_2,\cdots,o_i\}$为主体施加操作的对象的集合，如文件、数据、程序。

定义 3 节点集合 N

$N=\{n_1,n_2,\cdots,n_i\}$，节点包括终端节点和服务器节点，但 $e,q,g\notin N$。

定义 4 节点凭证集合 C

$C=\{c_1,c_2,\cdots,c_i\}$为各节点合法性的唯一凭证。节点凭证包括节点的物理地址、安全属性和所属部门等信息。

定义 5 安全级别 L

$L=\{(lc,lk), lc\in Lc, lk\subseteq Lk\}$，其中，$Lc=\{lc_1, lc_2,\cdots, lc_i\}$为安全等级集合，对 $\forall a,b\in Lc$，$a>b$ 表示安全等级 a 高于安全等级 b；$Lk=\{lk_1,lk_2,\cdots,lk_i\}$表示安全范畴的集合。设 $l_1=(lc_1,lk_1)$，$l_2=(lc_2,lk_2)$，安全级别 l_1 支配 l_2，当且仅当 $lc_1\geqslant lc_2$、$lk_1\supseteq lk_2$，记作 l_1 dom l_2。

定义 6 访问模式集合 A

$A=\{x|x=(r,w)\}$，其中，r 表示读操作；w 表示写操作。与多级安全操作系统不同，在网络信息共享情形中，主要关注网络信息的读写操作。

定义 7 通信关系集合 T

令 $N'=N\cup\{e,q,g\}$，$T\subset N'\times N'$ 表示实体的通信关系，$(a,b)\in T$ 表示 a 与 b 的通信，(a,b)为单向有序对，$|(a,b)|=1$ 表示实体的直接通信关系，即 a 可向 b 直接发送数据，$|(a,b)|\neq 1$ 表示 a 不可向 b 直接发送数据。

定义 8 传输路径 H

$H(a,b)=\{h_i(a,b)\}$，表示从 a 到 b 的所有实体集的集合，其中，$h_i(a,b)=\{z_k\,|\,(z_k,z_l)\in T$ and z_k 构成 T 的一条路径, $z_k\neq z_l, 1\leqslant k,l\leqslant m, a=z_1, b=z_m\}$，表示从 a 到 b 的某条可传输路径上的实体集合(实体为 N' 中的元素)。

定义 9 安全标记函数 F

$F=\{(f_s,f_o,f_n)\}$，其中：

(1) $f_s: S\to L$ 为主体安全标记函数；

(2) $f_o: O\to L$ 为客体安全标记函数；

(3) $f_n: N\to L$ 为节点安全标记函数。

定义 10 证书获取函数 CG

$CG: S\to C$，对 $\forall n\in N$，$CG(n)=c$，$c\in C$ 为节点 n 的凭证；若 $CG(n)=\phi$，表示证书获取失败。

定义 11 接入认证函数 EA

$EA: C\to D$，其中，$D=\{$yes, no, error$\}$，表示对节点是否允许接入网络的判定，对 $\forall c\in C$：(1)$OE(c)$=yes，表示接入认证通过；(2)$OE(c)$=no，表示接入认证失败；(3)$OE(c)$=error，表示接入认证出错。

定义 12 客体密级标定函数 OE

$OE: O\to L$，对 $\forall o\in O$，$OE(o)=l$ or ϕ，其中，$l\in L$ 为客体 o 的安全级别；ϕ 表示客体 o 的密级标定出错。OE 对客体进行内容检查，提取客体的特征向量，通过与各安全级别的特征向量比较评估出客体的安全级别。

令 $B\subseteq S\times O\times A$ 表示当前访问集合，$\boldsymbol{M}$ 为当前状态下的访问控制矩阵，$\boldsymbol{M}$ 中的元素 M_{ij} 是主体 s_i 对客体 o_j 的访问权限集合。

定义 13 系统状态集合 $V\subseteq(B\times\boldsymbol{M}\times F\times N)$

在 MLS-LAN 中，节点接入、密级标定和信息共享等操作都会引起系统状态迁移。

2.2 模型安全规则

为保证网络环境下信息共享的安全，需要从源头建立安全机制，全面而细致地实施节点间访问控制。本文针对节点接入、信息密级标定、信息共享和通信关系控制，设计了如下 4 条规则。

规则 1 接入认证规则

在$(B,\boldsymbol{M},F,N)$状态下，$n_i\in N$ 请求接入网络，其节点凭证为 $CG(n_i)$，对节点接入的处理如下：

(1)若 $CG(n_i)=\phi$，则拒绝节点接入。

(2)若 $CG(n_i)=c_i$，$EA(c_i)$=yes，则：

1)构造 F^*，使得：

$F^*=\{f_n(n_i)\}\cup F$

2)构造 N^*，使得：

$N^*=\{n_i\}\cup N$

3)系统进入状态 V^*：

$V^*=(B,\boldsymbol{M},F^*,N^*)$

(3)若 $EA(c_i)$=no or error，则拒绝节点 n_i 接入。

规则 1 描述了系统添加节点的接入认证规则以及由此引起的系统状态迁移，要求必须是合法的节点才可以接入网络，c_i 作为网络接入认证的唯一凭证，对接入认证的结果起决定性作用。

规则 2 密级标定规则

在$(B,\boldsymbol{M},F,N)$状态下，对于属于主体 s_i 的客体 $o_j\in O$，若共享时未知 o_j 的安全级别，则必须标定 o_j 的安全级别，令 $\delta(o_j)$ 表示 o_j 的特征向量集合，对 $\forall s\in S$，(s,o_j,x)表示主体 s 请求对客体 o_j 进行“x”访问。根据函数 OE，对 o_j 密级标定的处理如下：

(1)若 $\delta(o_j)=\phi$，则认为特征向量提取失败，禁止所有(s, o_j, x)的操作。

(2)若 $\delta(o_j)\neq\phi$，$OE(o_j)$ dom $f_s(s_i)$，则：

1)构造 F^*，使得：

$$F^*=\{f_o(o_i)\}\cup F$$

2)系统进入状态 V^*：

$V^*=(B,\boldsymbol{M},F^*,N)$

(3)若 $OE(o_j)=\phi$，则禁止所有(s,o_j,x)的操作。

(4)若 $OE(o_j)$不支配 $f_s(s_i)$，则 $OE(o_j)$无效。

规则2描述了对客体 o_j进行密级标定的过程以及由此引起的系统状态迁移，要求未知安全级别客体在共享时都必须通过信息密级标定。对于系统中存储的静态资源，安全管理员可根据资源标识划分密级，直接进行机密性控制；而动态资源的数据内容是由通信双方任意约定的，为控制动态资源的共享，规则2对动态资源进行密级标定，并规定客体的安全级别必须支配其所属主体的安全级别，由此解决了动态客体资源共享的安全问题。

规则3 信息共享规则

在$(B,\boldsymbol{M},F,N)$状态下，$\forall s_i\in S$，$\forall o_j\in O$，$x\in A$，对(s_i, o_j, x)的处理如下：

(1)当 $x=r$ 时，若 $f_s(s_i)$ dom $f_o(o_j)$，则：

1)对(s_i,o_j,r)操作进行授权，构造 B^*，使得：

$$B^*=\{(s_i,o_j,r)\}\cup B$$

2)系统进入 V^*状态：

$V^*=(B^*,\boldsymbol{M},F,N)$

3)若 $f_s(s_i)$不支配 $f_o(o_j)$，则拒绝(s_i,o_j,r)操作。

(2)当 $x=w$ 时，若 $f_o(o_j)$ dom $f_s(s_i)$，则：

1)对(s_i,o_j,w)操作进行授权，构造 B^*，使得：

$$B^*=\{(s_i,o_j,w)\}\cup B$$

2)系统进入 V^*状态：

$V^*=(B^*,\boldsymbol{M},F,N)$

3)若 $f_o(o_j)$不支配 $f_s(s_i)$，则拒绝(s_i,o_j,w)操作。

规则3描述了信息客体在主体之间传输的状态迁移规则，即(s_i,o_j,x)操作在不破坏 BLP 模型中 ss-特性和*-特性的前提下的状态迁移过程。

令集合 $K\subseteq N'$，$K\lhd(a,b)$ 表示 K 中的实体可以控制 a、b 之间的通信关系，那么对 $\forall h_i(a,b)\subseteq H(a,b)$，有 $K\subseteq h_i(a,b)$。由定义8可知，若能控制 $H(a,b)$中的所有节点，即可控制由 a 到 b 的数据传输过程。

规则4 通信关系控制规则

对 $\forall a,b\in N$，$a\neq b$，有 $K_1=\{a,b\}$，令 $K_2\subseteq N'$，$K_1\cap K_2=\phi$，若存在 a 与 b 之间的通信，则有 $K_2\lhd(a,b)$，且 $q,g\in K_2$。

规则4描述了 MLS-LAN 内节点间的通信关系控制规则，规定任意两节点间的通信必须受除通信双方外的一些节点或部件的控制，且 q 和 g 在控制部件之列。

3 模型安全性分析

本节将证明 MLS-LAN 模型的安全性，并依据规则2~规则4分析 MLS-LAN 安全模型中的信息流。

3.1 模型的安全性证明

命题1 规则1是保持状态安全的。

证明：令初始状态 V 是安全的，若 $CG(n_i)=\phi$ 或 $EA(c_i)=$ no 或 $EA(c_i)$=error，则 $F^*=F$，$N^*=N$，$V^*=V$ 必然为安全的。若 n_i 被授权接入网络，则 $F^*-F=\{f_n(n_i)\}$，$N^*-N=\{n_i\}$。n_i 被验证为合法节点，后续所有关于 n_i 的操作均遵守本文提出的安全规则和 BLP 模型中的安全规则(下文会证明规则2~规则4是安全的)，所以，V^*为安全状态。

命题2 规则2是保持状态安全的。

证明：令初始状态 V 是安全的，若 $\delta(o_j)=\phi$ 或 $OE(o_j)=\phi$ 或 $OE(o_j)$不支配 $f_s(s_i)$，则 $V^*=V$ 保持安全状态。反之，$F^*-F=\{f_o(o_i)\}$，$V^*-V=\{f_o(o_i)\}$，状态中只是增加了客体 o_i 的安全标记函数 $f_o(o_i)$，并没有破坏系统其他状态，对 o_i 仍按照 BLP 模型的安全规则进行操作，所以，规则2保持了安全状态。

命题3 规则3是保持状态安全的。

证明：令初始状态 V 是安全的，若(s_i,o_j,x)被拒绝，则 $V^*=V$，显然保持安全状态；否则，$B^*-B=\{(s_i, o_j,x)\}$或 ϕ，若为 ϕ，则有 $\{(s_i,o_j,x)\}\in B$，V^*为安全的；若不为 ϕ，规则3中的条件都满足 BLP 模型的 ss-属性和*-属性，综上，V^*是安全的，即规则3是保持状态安全的。

3.2 MLS-LAN 信息共享的安全性分析

依据规则4可得出下述2个命题：

命题4 对 $\forall a,b\in N$，a、b 两节点之间不可直接连接，即 $|(a,b)|\neq 1$。

证明：反证法。

假设 $|(a,b)|=1$，则 $\{a,b\}\subseteq H(a,b)$，根据规则4，由于 $K_1\cap K_2=\phi$，因此 $\{a,b\}\cap K_2=\phi$，由 $K_2\lhd(a,b)$ 及 K 的定义可知，对 $\forall h_i(a,b)\subseteq H(a,b)$，有 $K_2\subseteq h_i(a,b)$，则：

$$K_2\cap h_i(a,b)\neq\phi$$

可得：

$$\{a,b\}\cap K_2\neq\phi$$

两者矛盾，因此命题4得证。

命题5 对 $\forall a,b\in N$，a、b 两节点之间通信必然经过 q 和 g，即对 $\forall h(a,b)\subseteq H(a,b)$，有 $\{q,g\}\subseteq h(a,b)$。

证明：反证法。

假设 $\{q,g\}\not\subset h(a,b)$，依据规则4，由 $q,g\in K_2$ 可得：$\{q,g\}\subseteq K_2$，且 $K_2\lhd(a,b)$，由 K 的定义可知 $K_2\subseteq h(a,b)$，即得出 $\{q,g\}\subseteq h(a,b)$，与上述假设矛盾，命题5得证。

命题4表明，MLS-LAN 中任意两节点不可直接连接，命题5则表明节点间的通信必须经过 q 和 g。

在 MLS-LAN 中，α_1 和 α_2 表示不同节点中的主体，Lo_i 表示 o_i 的安全级别，D_m 表示是否允许信息共享的判定。假设节点 a 和节点 b 为合法节点，节点 a 中的主体 α_1 向节点 b 中主体 α_2 传输客体 o_i，其过程如下：

$$\alpha_1\rightarrow g:o_i,\alpha_2;$$

$g \rightarrow q$: o_i;

q:

$OE(o_i)= Lo_i$;

$q \rightarrow g$: Lo_i;

g:

if $f_s(\alpha_2)$ dom $f_o(o_i)$, D_m=yes;

else D_m=no;

$g \rightarrow \alpha_2$:

if D_m=yes, Send(o_i);

else Discard(o_i)

对于 (α_1,α_2) 共享客体 o_i，首先将 o_i 发送至 g，由 g 将客体 o_i 转发给 q，然后 q 为客体 o_i 标定安全级别，将标定的 Lo_i 反馈给 g，g 根据主客体安全标记实施访问控制，然后依据访问控制结果决定是否将 o_i 发送给 α_2。

命题 6 MLS-LAN 中信息共享过程是安全的。

证明：令信息共享之前的状态 V 是安全的，$\alpha_1 \rightarrow g$、$g \leftrightarrow q$ 和 $g \rightarrow \alpha_2$ 表明信息共享路径满足命题 5 中所述的 $\{q,g\} \subseteq h(a,b)$，其中，q 中数据处理过程满足规则 2，而 g 中对信息共享的处理满足 ss-属性和*-属性，综上，MLS-LAN 信息共享的过程均满足 2.2 节所描述的规则，根据命题 1~命题 3，可知该过程可保持系统的安全状态。

4 结束语

本文首先分析了局域网面临的威胁和几种多级安全模型、安全部署架构的不足，在此基础上提出一种面向局域网的多级安全模型 MLS-LAN。该模型针对局域网络环境下信息共享的多级安全需求，通过增加接入认证、密级标定和信息共享等控制规则，分别在网络节点接入和主体间信息共享过程等环节建立了安全机制，并由通信关系控制规则推导出网络节点连接和节点间信息传输路径的约束条件，确保对网络信息共享实施可靠的访问控制，提高局域网中信息共享的安全性。

参考文献

[1] Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria(Orange Book)[M]. Washington D. C., USA: [s. n.], 1985: 50-53.

[2] Kang M H, Froscher J N, Moskowitz I S. An Architecture for Multilevel Secure Interoperability[C]//Proc. of Computer Security Applications Conference. [S. l.]: IEEE Press, 1997.

[3] Irvine C E, Nguyen T D, Shifflett D J, et al. MYSEA: The Monterey Security Architecture[C]//Proc. of the Workshop on Scalable Trusted Computing. [S. l.]: ACM Press, 2009.

[4] 司天歌，张尧学，戴一奇. 局域网中的 L-BLP 安全模型[J]. 电子学报, 2007, 35(5): 1005-1008.

[5] 孟祥义. 多级安全网络研究[D]. 西安: 西安电子科技大学, 2008.

[6] Bell D E, LaPadula L J. Secure Computer System: Unified Exposition and Multics Interpretation[R]. The MITRE Corporation, Tech. Rep.: ESD-TR-75-306, 1976.

[7] Bell D E. Looking Back at the Bell-LaPadula Model[C]//Proc. of the 21st Annual Computer Security Applications Conference. [S. l.]: IEEE Press, 2005.

编辑 张 帆

(上接第 140 页)

5 结束语

基于 HVS 抗统计分析的小波域密写会导致小波系数直方图出现异常。针对这一特点，本文提出小波系数统计特征量分析法。分析及实验结果表明，本文方法能有效检测出秘密信息的存在性，并且在不同嵌入率下均表现出良好的性能。但是该方法不能估计出秘密信息的嵌入量，在后续工作中将寻求估计秘密信息嵌入量的方法。

参考文献

[1] 刘 劲, 康志伟, 何怡刚. 一种基于小波对比度和 LSB 的密写[J]. 电子学报, 2007, 35(7): 1391-1393.

[2] Cheddad A, Condell J, Curran K. Digital Image Steganography: Survey and Analysis of Current Methods[J]. Signal Processing, 2010, 90(3): 727-752.

[3] Zhang Xingpeng, Wang Shuozhong. Steganography Using Multiple-base Notational System and Human Vision Sensitivity[J]. IEEE Signal Processing Letters, 2005, 12(1): 67-70.

[4] Lou Der-Chyuan, Wu Nan-I, Wang Chung-Ming. A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity[J]. Journal of Systems and Software, 2010, 83(7): 1236-1248.

[5] Machado R, Noda H, Spaulding J. Application of Bit-plane Decomposition Steganography to JPEG2000 Encoded Images[J]. IEEE Signal Processing Letters, 2002, 9(12): 410-413.

[6] Tortes-Maya S, Nakano-Miyatake M, Perez-Meana H. An Image Steganography System Based on BPCS and IWT[C]//Proc. of the 16th International Conference on Electronics, Communications and Computers. [S. l.]: IEEE Press, 2006: 51-57.

[7] 康志伟, 刘 劲, 何怡刚. 基于 HVS 的抗统计分析的小波域密写[J]. 国防科学技术大学学报, 2007, 35(7): 1391-1393.

[8] Fridrich J, Goljan M, Du Rui. Detecting LSB Steganography in Color and Grey-scale Images[J]. IEEE Multimedia, 2001, 8(4): 22-28.

编辑 张 帆