局域网络中的 L-BLP 安全模型

司天歌,张尧学,戴一奇
(清华大学计算机科学与技术系,北京 100084)

摘 要: 为解决分布式网络环境下的机密性控制问题,本文提出一种 BLP 安全模型在局域网中的扩展模型 L-BLP. 通过在系统中增加动态监控单元,定义其拓扑结构,并构造了新的状态转换规则,实现对主体间通信行为的控制. 分析表明,L-BLP 模型可解决局域网内数据的机密性控制问题,并进行了安全性证明.

关键词: 计算机网络安全; BLP 安全模型; 访问控制
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0372-2112 (2007) 05-1005-04

L-BLP Security Model in Local Area Network

SI Tian-ge, ZHANG Yao-xue, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: As an extension of BLP in local area network, L-BLP model was developed to enforce information confidentiality in distributed network environment. It can control communications between subjects by adding dynamic monitor units into system, defining system topology and constructing new state transition rules. Analyses prove the security of L-BLP model and show that it can solve information confidentiality problems.

Key words: computer network security; BLP security model; access control

1 引言

信息的私密性保护与访问控制是各种安全隐患中的重要问题之一,尤其在网络信息系统中,信息泄露与非法访问行为的发生更加容易,而防范则更加困难. 根据 2006 年 CSI/FBI 公布的调查报告[1],由于信息的非法访问与泄露造成的经济损失之和在各类计算机安全问题所造成的经济损失中位居第一. 另一方面,美国总统的信息技术顾问委员会 2005 年发布的报告指出[2],由于网络的复杂性不断增强,系统的内部与外部已难以区分,所以应改变传统的基于内外边界防御的观念,扩大安全防御的范围,把网络的内部作为安全防御的重要领域,将局域网内的主体与局域网外的主体一视同仁. 本文基于 Bell-LaPadula (BLP) 安全模型[3~6],提出一种基于局域网的 BLP 扩展模型 (L-BLP),以解决网络环境下尤其是局域网系统内的信息泄露与访问控制问题.

2 BLP 模型及其网络应用

2.1 BLP 安全模型

BLP 模型是一个状态机模型,它定义了系统状态和系统各状态间的转换规则,规定了一组用于约束系统状态转换规则的安全公理,并证明了系统的安全性,即在其约束规则下转换的系统如果初始状态安全,则系统是安全的. BLP 模型的形式化描述如下.

(1) S 是主体集合, S_T 是可信主体集合, $S' = S - S_T$, O 是客体集合, A 是访问方式集合, C 是等级集合, K 是类别集合,敏感标记集合 $L = C \times K$,并定义 L 上的二元关系 $\geq$,对 $L_1 = (C_1, K_1)$, $L_2 = (C_2, K_2)$, $L_1 \geq L_1 := (C_1 \geq C_2) \wedge (K_1 \supseteq K_2)$. 系统状态集合 $V = B \times M \times F \times H$, $B = P(S \times O \times A)$ 为当前访问集合, $M = \{M_k\}$ 为访问矩阵集合, M_k 中元素 M_{ij} 表示 s_i 对 o_j 的访问方式, $F = L^S \times L^O \times L^S = \{(f_S, f_O, f_C) \mid \forall s \in S, f_S(s) \geq f_C(s)\}$ 为敏感标记函数集合, f_S 是主体最大敏感标记函数, f_O 是客体敏感标记函数, f_C 是主体当前敏感标记函数, H 是客体层次关系集合.

(2) 系统状态 v 是安全状态 iff v 满足以下三个安全特性.

简单安全特性(ss-特性) 状态 $v = (b, M, f, H)$ 满足 ss-特性 iff $\forall (s, o, x) \in b, x = r$ 或 $w \Rightarrow f_S(s) \geq f_O(o)$

*** - 特性** 状态 $v = (b, M, f, H)$ 满足 * - 特性 iff $\forall (s, o, x) \in b, s \in S', (a)\ x = r \Rightarrow f_C(s) \geq f_O(o)$; $(b)\ x = a \Rightarrow f_O(o) \geq f_C(s)$; $(c)\ x = w \Rightarrow f_C(s) = f_O(o)$

收稿日期:2006-12-28;修回日期:2007-03-14
基金项目:国家自然科学基金(No. 60673065);国家 863 高技术项目(No. 2005AA114160)

自主安全特性(ds-特性) 状态 $v=(b,M,f,H)$ 满足 ds-特性 iff $\forall(s_i,o_j,x)\in b \Rightarrow x\in M_{ij}$

(3) 状态转换规则定义为 $\rho: R\times V\rightarrow D\times V$, R 是请求集合, D 是判定集合,判定的结果为 Yes、No 或 ?,分别表示请求被执行、被拒绝或请求不能被处理. 规则 $\rho(R_k,v)=(D_m,v^*)$ 保持安全状态 iff 状态 v 与 v^* 是安全状态.

(4) 基本安全公理:如果系统的初始状态是安全的,而状态转换是在转换规则的约束下进行的,则从初始状态开始的任何状态都是安全的.

2.2 BLP 模型在网络应用中的局限

BLP 模型的形式化描述同时给出了建立 BLP 应用的基本思路:需要确定主体和客体,为它们分配安全标记,并根据安全标记与访问权限控制矩阵监控主体对客体的每一次访问行为,以确保该行为都符合 BLP 的安全特性. 在此过程中,最重要的问题是如何确保每次访问都要经过系统的检查. 对局域网而言,由于自身缺乏集中控制机制,所以在防泄密方面具有很大的局限性:(1) 网络内主机具有自主性,其它主机无法监控其内部的行为;(2) 网络拓扑结构的多样容易导致泄密,如对总线式网络拓扑结构可进行网络监听非法获取数据;(3) 网络内主机之间的通信协议灵活多样,无法针对所有协议进行防护,使得泄密行为更加难以控制.

目前,Labeled Networks (LN)、Multiple Independent Levels of Security(MILS) 等基于 BLP 模型的安全系统被提出以保护局域网环境下的信息安全[7]. 其中,LN 重新设计了网络内主机间的通信协议,在通信报文头部携带密级信息,系统根据双方密级情况决定是否授权每次的信息交换而实现安全保护,但由于 LN 采用专用协议,因此通用性较差. MILS 为网络内的每个主机分配固定的密级,根据主机密级的不同把网络划分为多个子网,并设置专用的多级服务器来连接多个子网,低密级网络内的主机在服务器上存储数据,高级别网络内的主机访问该服务器获取数据从而实现信息交换. MILS 实际上是以不同密级的子网作为主体,无法对主机进行保护,同时,MILS 要求相同级别的主机处于独立的子网中,限制了网络的物理分布.

本文提出了 L-BLP 模型,在局域网中引入动态监控设备和资源服务器,实现集中控制机制,以保护网络内的机密数据.

3 L-BLP

3.1 模型描述

3.1.1 符号定义

L-BLP 系统可形式化地表示为 $(\mathbb{C},G,P,W)$,其中:

(1) $\mathbb{C}=\{c_i\}$ 表示计算机的集合, c_i 表示单台计算机,若 $|\mathbb{C}|=1$,则表示该系统由单台计算机组成. 令元素 $\hat{e}$ 表示与该局域网互通的外部网络,并将其视作一个特殊的计算机,如果 L-BLP 与外网相连,则 $\hat{e}\in\mathbb{C}$,否则 $\hat{e}\notin\mathbb{C}$.

(2) $G=\{g_i\}$ 表示动态监控设备集合.

(3) $P=\{p_i\}$ 表示资源服务器集合.

(4) $W\subseteq(\mathbb{C}\cup G\cup P)\times(\mathbb{C}\cup G\cup P)$,表示实体的直接通信关系. 对 $\forall a,b\in\mathbb{C}\cup G\cup P$, $(a,b)\in W$ 表示 a 可向 b 直接发送数据, $(a,b)\notin W$ 表示 a 不可向 b 直接发送数据. (a,b) 是有序对,并规定 $(a,a)\in W$.

(5) $(a,*)=\{x|(a,x)\in W, x\in\mathbb{C}\cup G\cup P\setminus\{a\}\}$, $(*,a)=\{x|(x,a)\in W, x\in\mathbb{C}\cup G\cup P\setminus\{a\}\}$ 分别表示可与 a 直接通信的设备集合.

根据以上符号,系统的主体、客体以及 G 与 P 的功能描述如下.

(1) 主体:在局域网中,从整个系统的角度很难监控某个主机上的进程活动,即使以某种技术手段实现,也会极大地降低整体性能. 所以,L-BLP 把网络中的每个主机作为一个受控的主体,即系统的主体集合 $S=\mathbb{C}$.

(2) 客体:L-BLP 控制的资源包括两部分:一部分是静态资源,包括主体需要的各种程序和数据文件目录等静态信息;另一部分是动态资源,即主体之间的通信数据. 对于静态资源,管理员可以直接根据资源标识划分密级,把资源作为客体直接进行机密性控制,但必须要求这些资源位于主体之外,否则将无法对这部分客体进行监控,同时,这也满足了应用中提出的重要数据进行集中管理的需求. 因此,可将这部分静态数据集中存放于集合 P 的元素中. 对于动态资源,系统无法对内容未知的通信数据划分密级,但可转为对可划分密级的通信行为(即通信关系)进行控制. 综上,客体集合 $O=W\cup\{p_i$ 对外提供的数据$\}$.

(3) 在 L-BLP 中,由 G 与 P 共同监控主体对客体的访问: G 负责控制主体对客体中动态部分(即通信关系)的访问行为, g_i 与交换机设备类似,可连接多个主体完成它们之间的数据转发工作,同时, g_i 记录所有主体的敏感标记信息,并根据主体的敏感标记信息,动态地决定主体之间的通信关系; P 负责控制主体对静态客体资源的访问行为, p_i 需要记录自身存储的静态资源的敏感标记信息,并根据主体和客体的敏感标记以及 BLP 的安全属性来决定是否授权主体对客体的访问行为.

3.1.2 状态转换规则

BLP 系统是一个状态机模型,系统通过状态转换规则进行状态转换,同时,状态转换规则也描述了系统的工作过程. 文献[5]提出了 10 条状态转换规则,对其安

全性进行了证明. 在L-BLP中,访问控制矩阵、静态客体资源、主客体的敏感标记等信息分别保存在新的实体 G 和 P 中,并且,系统还要控制主体之间的动态客体资源,因此,L-BLP在进行状态转换时,需要提出新的状态转换规则,而不能直接使用原有的状态转换规则.

令 ρ^0 表示原有的状态转换规则,$\hbar$ 表示请求的数据,$\hbar'$ 表示对应 $\hbar$ 的响应数据,σ_2 与 σ_1 表示主体,R_k 和 D_m 分别表示任意的请求与判定,其余符号参见文献[5].

规则1　σ_2 对 P 上存储的客体访问:$\rho^1(R_k, v) \equiv$

(1) $\sigma_2 \rightarrow G:\hbar$

(2) $G \rightarrow P:\hbar$,if $\sigma_1 \neq \phi$ then $\{f_S(S\lambda), f_C(S\lambda)\}$,if $\sigma_2 \neq \phi$ then $\{f_S(S_i), f_C(S_i)\}$

(3) $P:\rho^0(R_k, v) = (D_m, v^*)$

(4) $P \rightarrow G \rightarrow \sigma_2$:if $(D_m = \text{yes})$ then $\hbar'$

规则2　σ_2 向 σ_1 经过 G 传输 P 上静态客体:$\rho^2(R_k, v) \equiv$

(1) $\sigma_2 \rightarrow G: O_j, \sigma_1$

(2) $G \rightarrow P: O_j$,if $\sigma_1 \neq \phi$ then$\{S\lambda\}$,if $\sigma_2 \neq \phi$ then$\{S_i\}$

(3) $P \rightarrow G: M_{ij}, M_{\lambda j}$

(4) G:

if $(\sigma_1 = \phi)$ or $(\sigma_2 = \phi)$ or $((x \neq r)$ and $(x \neq a))$

then $\rho^2(R_k, v) = (?, v)$

if $(x \notin M_{ij})$ or $(x \notin M_{\lambda j})$

then $\rho^2(R_k, v) = (\text{no}, v)$

if $(f_C(S\lambda) \geq f_C(S_i))$

then $\rho^2(R_k, v) = (\text{yes}, augb(R_k, v))$

else $\rho^2(R_k, v) = (\text{no}, v)$

end.

(5) $G \rightarrow \sigma_1$:if $(D_m = \text{yes})$ then O_j

规则1描述了系统在主体对静态客体访问时的处理流程,即所有的主体与资源服务器的数据通信必须经过 G, G 在数据交换时将主体的敏感标记信息交付给资源服务器,再由资源服务器根据 ρ^0 处理完成状态转换.

规则2描述了 P 上存储的静态客体资源在主体之间传输的状态转换规则,而在局域网中,主机之间还会传输更多其它的数据,即动态客体资源,这些数据的内容是由通信双方任意约定的,系统很难区分这些数据是静态客体还是动态客体,因而无法控制此传输过程. 并且,局域网内主机间的点对点通信更普遍,这种经过 P 中转的数据交换大大地降低了系统性能. 规则3将对主体之间发生的两两数据交换过程进行控制.

规则3　σ_2 向 σ_1 进行数据通信:$\rho^3(R_k, v) \equiv$

定义二元关系 $L \subseteq S \times S$, $L = \{(S_i, S_j) \mid \forall O_k \in O, (x \in M_{ik}) \wedge (x \in M_{ik}), x = a$ 或 $w\}$,显然,L 满足自反、对称和传递性,是 S 上的等价关系. 因此,令商集 S/L 表示对 S 的一个划分.

(1) $\sigma_2 \rightarrow G:\hbar, \sigma_1$

(2) G:

if $(\sigma_1 = \phi)$ or $(\sigma_2 = \phi)$ or $((x \neq r)$ and $(x \neq a))$

then $\rho^2(R_k, v) = (?, v)$

if $(f_C(S\lambda) \geq f_C(S_i))$ and $(S\lambda \in [S_i]_L)$

then $\rho^2(R_k, v) = (\text{yes}, augb(R_k, v))$

else $\rho^2(R_k, v) = (\text{no}, v)$

end.

(3) $G \rightarrow \sigma_1$:if $(D_m = \text{yes})$ then $\hbar'$

规则3把主体按照对客体的访问权限不同进行分组,若同组的主体满足规则3中敏感标记的规定,则可以进行数据通信,而不同组的主体之间不能进行数据通信. 考虑到在实际应用环境中,系统通常会根据主体对客体的访问权限进行用户分组,所以,规则3的要求是合理的.

3.1.3　拓扑结构

规则1、2、3要求系统内所有主体的数据通信行为都经过 G,这就需要对L-BLP系统的拓扑结构进行分析.

令 $e_i(a, b) = \{z_k \mid (z_k, z_l) \in W$ 且 z_k 构成一条路径,$z_k \neq z_l, 1 \leq k, l \leq m, a = z_1, b = z_m\}$,表示从 a 到 b 的某条可传输数据的路径上的节点集合. $E(a, b) = \{e_i(a, b)\}$,表示从 a 到 b 的所有节点集的集合. 显然,$e_i(a, b)$ 中的元素可在该路径上控制从 a 到 b 的数据传输,进而,如果在所有路径上都能控制从 a 到 b 的数据传输,则将控制 a、b 之间的通信关系. 因此,对集合 $Z \subseteq \mathbb{C} \cup G \cup P$,定义 $Z \triangleright (a, b)$ 表示 Z 中的实体可以控制主机 a、b 之间的通信关系,即对 $\forall e_i(a, b) \in E(a, b)$, $Z \cap e_i(a, b) \neq \varnothing$.

根据以上符号,可得到如下结论.

命题1　对非空集合 $Z_1, Z_2 \subset \mathbb{C} \cup G \cup P$, $Z_1 \cap Z_2 = \varnothing$,若对所有 $a, b \in Z_1, a \neq b$,均有 $Z_2 \triangleright (a, b)$,则 $(a, b) \notin W$.

证明　用反证法. 若 $\exists b \in Z_1$ 满足 $(a, b) \in W$,则根据 $E(a, b)$ 定义有 $\{a, b\} \in E(a, b)$,因为 $Z_1 \cap Z_2 = \varnothing$,所以 $\{a, b\} \cap Z_2 = \varnothing$,但由 $Z \triangleright (a, b)$ 定义得到 $\{a, b\} \cap Z_2 = \varnothing$,矛盾,从而得证.

命题2　若对所有的 $a, b \in \mathbb{C}, a \neq b$,均有 $((*, a) \cap P = (a, *) \cap P = \varnothing) \wedge (G \triangleright (a, b))$,则 $((a, *) \subseteq G) \wedge ((*, b) \subseteq G)$.

证明　用反证法. 若 $\exists c \in (a, *)$ 且 $c \notin G$,由已知 $(a, *) \cap P = \varnothing$,所以 $(a, c) \in W$ 且 $c \in \mathbb{C}$,即 $\{a, c\} \in$

$E(a,c)$,但由 $Z \triangleright (a,c)$ 定义得到$\{a,c\} \cap G \neq \varnothing$,所以命题得证.

推论 1 若对于 $\forall a,b \in \mathbb{C}, a \neq b, E(a,b) = \{e_i(a,b)\}$,均有若 $\cup(e_i(a,b) \setminus \{a,b\}) \subseteq G$,则 $G \triangleright (a,b)$.

证明 若 $\cup(e_i(a,b) \setminus \{a,b\}) \subseteq G$,则对 $\forall e_i(a,b) \in E(a,b)$ 且 $e_i(a,b) \neq \{a,b\}$,均有 $e_i(a,b) \subseteq G$,所以 $e_i(a,b) \cap G \neq \varnothing$,再由 $Z \triangleright (a,b)$ 定义,得证.

以上分析说明,若要 G 监控系统中主机间的通信,必须对网络拓扑结构进行限定. 命题 1 和命题 2 表明系统内的主机必须与 G 中元素直接相连,而不能互联;推论 1 则进一步指出,可以令 G 位于网络拓扑结构的中心位置,并使得主机之间的数据传输路径都经过 G 来构建 L-BLP.

3.2 安全性证明

规则 1 的安全性与 ρ^0 等价,即规则 1 保持安全状态. 下面证明规则 2 与规则 3 是保持状态安全的.

命题 3 规则 2 是保持状态安全的.

证明 令 v 是安全的,$R_k \in R, \rho^2(R_k, v) = (D_m, v^*)$,则 $v^* = v$ 或 $v^* = augb(R_k, v)$. 若 $v^* = v$,则 v^* 是安全的. 否则,$b^* - b = \{S_i, O_j, x\}$ 或 ϕ,若为 ϕ,则有 $\{S_i, O_j, x\} \in b$,v^* 是安全的. 若不为 ϕ,根据规则 2 有 $(f_C(S\lambda) \geq f_C(S_i)) \wedge ((x = r) \vee (x = a))$,此时,由于 $O_j \in b(S_i : r, a)$,则 $f_S(S\lambda) \geq f_C(S\lambda) \geq f_C(S_i) \geq f_O(O_j)$,即满足 ss-特性和 *-特性. 同时,由于 $(x \in M_{ij}) \wedge (x \in M_{\lambda\beta})$,规则 2 满足 ds-特性. 综上,$v^*$ 是安全的,即规则 2 是保持状态安全的.

命题 4 规则 3 是保持状态安全的.

证明 令 v 是安全的,$R_k \in R, \rho^3(R_k, v) = (D_m, v^*)$,则 $v^* = v$ 或 $v^* = augb(R_k, v)$. 若 $v^* = v$,则 v^* 是安全的. 否则,访问的客体 $b^* - b = \{S_i, r, x\}$ 或 ϕ,若为 ϕ,则有 $\{S_i, O_j, x\} \in b$,v^* 是安全的. 若不为 ϕ,先考虑 $\hbar$ 的构成,显然,$\hbar$ 可能包含当前 S_i 已经读取的多个客体数据,即在最复杂情况下,$\hbar = b(S_i : r, a)$,由规则 3 已知 $f_C(S\lambda) \geq f_C(S_i)$,则对 $\forall O_j \in b(S_i : r, a)$,均有 $f_S(S\lambda) \geq f_C(S\lambda) \geq f_C(S_i) \geq f_O(O_j)$,即满足 ss-特性和 *-特性. 同时,根据规则 3,$S\lambda \in [S_i]_L$,即 $(x \in M_{ij}) \wedge (x \in M_{\lambda\beta})$,所以规则 3 满足 ds-特性. 综上,$v^*$ 是安全的,即规则 3 是保持状态安全的.

4 结论

本文在局域网中对 BLP 模型进行扩展,提出了 L-BLP 模型. 该模型增加了对主体间通信行为的控制规则,针对局域网的特点,给出了描述主体间通信关系的拓扑结构的约束条件,并进行了安全性证明. 基于本文结果,我们已初步实现了一个实例系统,验证了其可行性和安全性. 当然在实际系统中,还需要考虑主体身份认证、通信安全以及抗抵赖等安全问题,但它们已超出本文的讨论范围.

参考文献:

[1] Lawrence A G,et al. 2006 CSI/ FBI Computer crime and security survey [R]. San Francisco, CA: Computer Security Institute,2006.

[2] President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization [R]. Arlington, Virginia: National Coordination Office for Information Technology Research and Development,2005.

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

[4] Bell D E,LaPadula L J. Secure computer system: Mathematical foundations [R]. Bedford, MA: Electronic Systems Dvision, Air Force System Command, Hanscom AFB,1973.

[5] Bell D E,LaPadula L J. Secure computer system: A mathematical model [R]. Bedford, MA: Electronic Systems Dvision, Air Force System Command, Hanscom AFB,1973.

[6] Bell D E. Looking back at the Bell-La Padula model [A]. Proceedings of the 21st Annual Computer Security Applications Conference [C]. Washington, DC: IEEE Computer Society, 2005. 337 - 351.

[7] Rick Smith. Introduction to multilevel security [EB/ OL]. http://www.cs.stthomas.edu/ faculty/ resmith/ r/ mls/ m3networks.html, 2005.

作者简介:

司天歌 男,1977 年生于辽宁,清华大学计算机科学与技术系博士生,主要研究方向为网络信息安全.

E-mail: sitg@theory.cs.tsinghua.edu.cn

张尧学 男,1956 年生于湖南,清华大学计算机科学与技术系教授,博士生导师,主要研究方向为计算机体系结构、计算机网络.

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.