Journal of Computer Applications
计算机应用,2013,33(3):717 -719,742
ISSN 1001-9081
CODEN JYIIDU
2013-03-01
http://www.joca.cn

文章编号:1001 -9081(2013)03 -0717 -03
doi:10.3724/SP.J.1087.2013.00717

跨域引用监视器及其以数据为中心的多级安全模型

李洪敏[1*],万平国[2],葛　杨[3]
(1.中国工程物理研究院 总体工程研究所,四川 绵阳 621900;
2.国际信息战略研究中心,北京 100094;　3.军工保密资格认证中心,北京 100094)
(*通信作者电子邮箱 lihm@caep.ac.cn)

摘　要:为基于不可信计算机系统来构建一个可信的多级安全(MLS)大系统,提出一种新型的跨域引用监视器及其多级安全模型。该跨域引用监视器采用现有的商业现货(COTS)产品,使用一个或多个独立的计算机,在两个或多个不同的网络之间,通过满足 EAL7 的单向传输硬件装置来连接。基于该跨域监视器实现了以数据为中心的多级安全模型。该模型允许信息从低密级网络流向高密级网络,也允许高密级网络把低密级数据发布给低密级网络,禁止高密级网络的高密级信息和无密级标记信息流向低密级网络,并已在分级保护的网络系统中成功应用。通过安全模型和安全策略的形式化描述和证明表明,基于该安全模型构建可信 MLS 大系统是可行的。

关键词:多级安全;引用监视器;安全模型;跨域;分级保护
中图分类号:TP393　**文献标志码**:A

Cross domain reference monitor and its data-centered multilevel security model

LI Hongmin[1*], WAN Pingguo[2], GE Yang[3]
(1. *Institute of System Engineering, China Academy of Engineering Physics, Mianyang Sichuan* 621900, *China*;
2. *Center of International Information Strategy Studies, Beijing* 100094, *China*;
3. *Center of Defense and Industrial Security Clearance Accreditation, Beijing* 100094, *China*)

Abstract: A new cross domain reference monitor and Multi-Level Security (MLS) model were proposed for a trusted MLS system. The model was based on Commercial Off-The-Shelf (COTS) products like commercial computers and security compliant hardware devices. System high networks were properly connected with reference validation computer by trusted one-way transfer devices (EAL7) for data-centric MLS model. The model allowed information to flow from low domain to high domain, and allowed sanitization data with low label to flow from high domain to low domain, but data without low label were prohibited to flow from high domain to low domain. The model was applied to the information system of classification protection. Formal verification of security model and policy demonstrates it is feasible for a MLS system with COTS products and trusted hardware devices.

Key words: Multi Level Security (MLS); reference monitor; security model; cross domain; cascade protection

0　引言

多级安全(Multi-Level Security, MLS)由文献[1]提出了近四十年,但目前的 MLS 技术、系统和解决方案远没有进入可用阶段。文献[2-4]认为,现行的信息安全措施,无论从实施效果上还是形式化证明上,被认为是"低安全",不能满足保障信息安全的需要。MLS 可以处理多种不同密级的信息,允许不同安全级别的用户,在控制知悉范围(Need to Know)的前提下,可以访问相应的信息并保障信息的安全,防止缺少授权用户有意或无意的访问。MLS 允许高安全级别的用户访问低密级的信息,也允许高安全级别的用户与低安全级别的用户共享低密级文档。

在计算机系统中,所有的数据是通过操作系统来访问的,因此安全操作系统是一个基础。文献[5]指出安全操作系统需要满足访问控制保护轮廓(Controlled Access Protection Profile, CAPP)、标记安全保护轮廓(Labeled Security Protection Profile, LSPP)和基于角色访问控制保护轮廓(Role-based Access Control Protection Profile,RBACPP)。现有的商用操作系统很难兼顾安全系统的标准,又满足应用需求。在市场上占统治地位的 Windows 操作系统更谈不上安全系统。

文献[6]认为没有安全操作系统的系统不安全,而安全操作系统难以实现,利用硬件来支持 MLS 这种想法开始得到支持。在嵌入式硬件上支持多个独立内核,使用多个独立的操作系统,文献[7]指出这就是多级独立安全系统(Multiple Independent Level of Security, MILS)。MILS 是 MLS 的一种特殊形式。一些实时嵌入式操作系统开始进军 MILS,但这类操作系统不是通用安全操作系统,基本不具备通用性。

美国海军 INSCOM 在 JWICS 和 SIPRNet 机密网中采用了 Oracle 的标签安全(Oracle Label Security, OLS)数据库、Trusted Rubix 和 SEPostgreSQL 数据库也支持 MLS。通用动力的可信网络环境(TNE)作为桌面环境支持 MLS。这些系统开始了初步应用,但认证还有待时日。

国内针对该课题的研究很少,国外近期的研究和相关应用表明,安全操作系统对 MLS 很重要,但并不是必需的。是一种充分而非必要的条件。因此本文在分析 MLS 安全问题的基础上,提出在不可信的计算机子系统上实现一个可信的大系统,它要求多个独立的计算机通过满足安全要求的硬件装置来连接。通过硬件来强制执行 MLS 的实例是光的单向

收稿日期:2012-09-25;**修回日期**:2012-11-19。

作者简介:李洪敏(1968 -),女,四川绵阳人,副研究员,CCF 会员,主要研究方向:网络与信息安全;　万平国(1964 -),男,北京人,研究员,主要研究方向:网络与信息安全;　葛杨(1957 -),男,北京人,研究员,主要研究方向:信息安全、安全检测。

传输装置。在该情形下,计算机和网络是 MSL(Multiple Single Level),但大系统是 MLS。

1 MLS 的安全问题

问题 1 高安全域向低安全域的信息发布问题。MLS 系统是以贝尔-拉帕杜拉(Bell-La Padula, BLP)模型为基础。BLP 模型规定了“不上读”“不下写”的安全属性。这是两个不能违反的安全属性。“向下写低密级信息”不会破坏保密性,但是无法给出形式化的证明。反过来说,“不下写”这个过于严格的安全属性,是 BLP 模型形式化证明的基础。MLS 继承了 BLP 模型的局限性和高安全级别的用户向低安全级别的用户共享低密级信息的难点。因此需要寻求一种有效、可靠的机制,来确保、验证信息是低密级的信息,是目前 MLS 要解决的问题之一。

问题 2 隐信道问题。文献[8]指出任何的双向通信,都无法给出隐信道消除的形式化证明。单向传输从低向高传输时,形式化证明不存在隐信道,但不能证明从高向低直接传输信息的保密性问题。另外单向传输的可靠性是一个问题,可靠性多是通过反馈来实现的,没有反馈意味着常用的可靠性机制无法使用。文献[9]通过数学方法已经将可靠性提升到可用的程度,在工程上已经不是问题。MLS 必须解决从高到低传输低密级信息时的保密性问题,至少要证明执行了强制访问可转换,没有或消除了隐信道。过去的四十多年的研究历史表明这是一件极为困难的事情。

问题 3 旁路问题。维基泄密是一个例子,旁路比隐信道的危害更大。旁路通常是由假设错误造成的。发现旁路,纠正它、避免它很容易,但要证明没有旁路则困难得多。

2 新型的跨域引用监视器设计

文献[10]在安德森报告中给出了引用监视器的概念,其示意图如图 1 所示。引用监视器使用了四十多年,从 TCSEC(1985)到 CC v2.1(1999)和 CC v3(2005)都采用了该框架,是可信计算机的评估基础。引用监视器定义一种引用验证机制,该验证机制满足三原则:不可篡改(tamperproofness)、始终调用(always invoked)和小到可分析(small enough to be analyzed)。

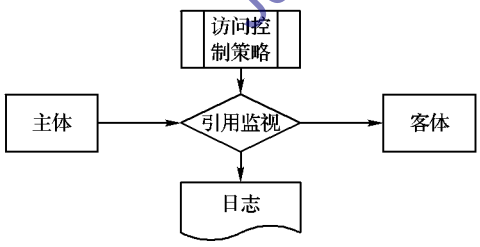

图 1 引用监视器示意图

本文提出一种新型的跨域引用监视器。该跨域引用监视器采用现有的商业现货产品,使用一个或多个独立的计算机,在两个或多个不同的网络之间,通过满足安全要求的单向传输硬件装置来连接,实现一个系统级的监视器,该系统具有引用监视器的全部安全特性。跨域引用监视器示图如图 2 所示。

自 1995 年美国海军研究实验室[11]提出网络泵(Network Pump)的概念来实现单向数据二极管(One Way Data Diode),文献[12]指出用了十多年的时间仍未能解决隐信道的问题。文献[13-14]证明了目前只有基于光的无反馈单向传输装置才解决单向传输的隐信道问题,达到了 CC 所能给出的最高认证 EAL7(中网、Tenix)。单向传输装置,解决了数据从低安全域流向高安全域的问题,但并没有解决数据从高安全域流向低安全的问题。单向传输装置不能用在从高安全域向低安全域发布数据,因为它破坏了 BLP 模型,也破坏了 MLS 的安全要求。而跨域引用监视器是一种能够满足 MLS 从高安全域向低安全域发布数据的安全模型。引用监视器的三原则:必须始终调用而不能绕过以保证仲裁的完整性;必须是防篡改的不被干涉以保证独立性;必须是可测试可分析,特别是对隐信道的测试和分析,以保证可证明和可证实。跨域引用监视器对传统的引用监视器的三原则给出了一个修正,即引用监视器应该足够简单,简单到可分析(simple enough to be analyzed)。本设计中的跨域引用监视器不小,甚至很大,但简单,简单到可分析,满足全部的形式化证明。

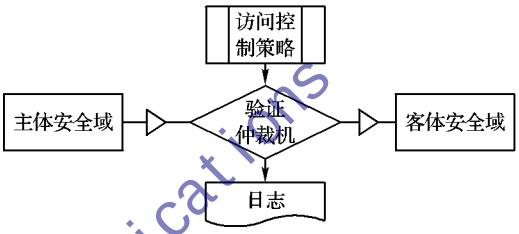

图 2 跨域引用监视器示意图

3 跨域引用监视器的安全性分析

定义 1 安全域初试状态划分为两个独立的安全域,其中:

1) 一个安全域,表示为 A;

2) 另一个安全域,表示为 B;

3) $\Leftarrow$ 表示信息的流向;

4) $\vdash(\neg(A \Leftarrow B)) \wedge (\neg(B \Leftarrow A))$

5) 即 A 和 B 两个安全域是物理隔离的。

定义 2 单向传输模型是一个三元组$(RX(A), TX(B), \Leftarrow)$,其中:

1) $RX(A)$ 表示在 A 安全域有一个接收模块;

2) $TX(B)$ 表示在 B 安全域有一个发送模块;

3) $\Leftarrow$ 表示信息的流向;

4) $\vdash(A \Leftarrow B) \wedge (\neg(B \Leftarrow A))$;

5) 即允许有 B 到 A 的信息流,但不能有 A 到 B 的信息流。

单向传输模型的形式化命题为:

$$\vdash(\exists TX \mid TX \in B)(\exists RX \mid RX \in A)(A \Leftarrow B) \wedge (\neg(\exists TX \mid TX \in A))(\neg(\exists RX \mid RX \in B))(\neg(L \Leftarrow H))$$

定义 3 信息流的保密性模型是一个四元组$(H, L, C, \Leftarrow)$,其中:

1) H 表示高安全域;

2) L 表示低安全域;

3) C 是一种 BLP 机制,表示 H 和 L 关系模型,H 对 L 是保密的,满足 BLP 保密性安全策略;

4) $\vdash(H \Leftarrow L) \wedge (\neg(L \Leftarrow H))$;

5) 即允许有 L 到 H 的信息流,但不能有 H 到 L 的信息流。

信息流的保密性模型的形式化命题为:$\vdash(H \Leftarrow L) \wedge (\neg(L \Leftarrow H))$。

定理 1 BLP 模型允许信息流通过单向传输装置从低安全域流向高安全域。

证明 根据定义 2,可得到 $\vdash(A \Leftarrow B) \wedge (\neg(B \Leftarrow A))$,

让 $A = H$ 和 $B = L$,则得到 $\vdash(H \Leftarrow L) \wedge (\neg (L \Leftarrow H))$。根据定义 3,所以命题成立。

定理 2　BLP 模型禁止信息流通过单向传输装置从高安全域流向低安全域。

证明　根据定义 2,可得到 $\vdash(A \Leftarrow B) \wedge (\neg (B \Leftarrow A))$,让 $A = L$ 和 $B = H$,则得到 $\vdash(L \Leftarrow H) \wedge (\neg (H \Leftarrow L))$。这明显与定义 3 矛盾,即违背了 BLP 模型。

定理 3　单向传输装置中接收方不可能干涉发送方。

证明　根据定义 2,可知 $\vdash(A \Leftarrow B) \wedge (\neg (B \Leftarrow A))$,假设 A 干涉 B,与 $(\neg B \Leftarrow A)$ 矛盾,所以命题成立。

定理 4　单向传输装置中发送方不可能推导接收方。

证明　根据定义 2,可知 $\vdash(A \Leftarrow B) \wedge (\neg (B \Leftarrow A))$,假设 B 想推导 A,与 $\neg (B \Leftarrow A)$ 矛盾,所以命题成立。

定理 5　单向传输装置满足失效也安全的属性。

证明　根据定义 2 可知,如果发生发送模块失效或接收模块失效,则 $\vdash(\neg (A \Leftarrow B)) \wedge (\neg (B \Leftarrow A))$。根据定义 1,两个安全域是物理隔离的,所以命题成立。

定义 4　跨域引用监视器模型是一个五元组 $(A, B, R, S, \Leftarrow)$,其中:

1) A 表示一个安全域,B 表示另一个安全域,且 $\vdash(\neg (B \Leftarrow A)) \wedge (\neg (A \Leftarrow B))$;

2) R 表示验证仲裁计算机;

3) S 表示信息的安全密级;

4) $\Leftarrow$ 表示信息的流向;

5) $\vdash(R \Leftarrow A) \wedge (\neg (A \Leftarrow R)) \wedge (B \Leftarrow R) \wedge (\neg (R \Leftarrow B))$;

6) 即允许安全域 A 的低密级信息 S 通过 R 流向安全域 B;但禁止安全域 B 的任何其他信息 S 通过 R 流向低安全域 A。

跨域引用监视器模型的形式化命题为:

$$\vdash(\exists S \mid S = L, S \in A)(R \Leftarrow A) \wedge (\forall S \mid S \in R)(\neg (A \Leftarrow R)) \wedge (\exists S \mid S = L, S \in R)(B \Leftarrow R) \wedge (\forall S \mid S \neq L, S \in R)(\neg (B \Leftarrow R)) \wedge (\forall S \mid S \in B)(\neg (R \Leftarrow B))$$

定理 6　跨域引用监视器允许高安全域的低密级信息流向低安全域。

证明　根据定义 4,让 $A = H$ 和 $B = L$,则 $\vdash(\exists S \mid S = L, S \in H)(R \Leftarrow H) \wedge (\exists S \mid S = L, S \in R)(B \Leftarrow R)$,所以命题成立。

定理 7　跨域引用监视器没有隐信道。

证明　根据定义 4,可知 $\vdash(\neg (B \Leftarrow A)) \wedge (\neg (A \Leftarrow B))$,即高安全域与低安全域物理隔离,而任何的隐信道的信号都属于无密级标识,由于 $\vdash(\forall S \mid S \neq L, S \in R)(\neg (B \Leftarrow R))$,即 R 禁止无密级标号的信号发送给低安全域,因此命题成立。

定理 8　跨域引用监视器没有旁路。

证明　如果存在旁路,则与 $\vdash(\neg (B \Leftarrow A)) \wedge (\neg (A \Leftarrow B))$ 矛盾,因此命题成立。

定理 9　跨域引用监视器是 MLS。

证明　根据定义 4,让 $A = H$ 和 $B = L$,可知 $\vdash(\neg (L \Leftarrow H)) \wedge (\neg (H \Leftarrow L))$,即高安全域不直接向低安全域下写,且 $\vdash(\forall S \mid S \neq L, S \in R)(\neg (L \Leftarrow R))$,即没有高密级信息或没有密级的信息通过跨域监视器流向低安全域,因此满足 BLP 模型。

4　以数据为中心的多级安全模型

本文给出基于跨域引用监视器实现的以数据为中心的多级安全模型的形式化描述。

设 $L(S) = l_s$ 是安全域 S 的安全密级,$L(O) = l_o$ 是数据客体 O 的安全密级,$C(S) = c_s$ 是安全域 S 的安全区间,$C(O) = c_o$ 是数据客体 O 的安全区间。对所有的安全密级 l_i 和 $c_s (i = 0, \cdots, k-1; l_i < l_{i+1}; c_i < c_{i+1})$。

定义 5　安全等级 (L_2, C_2) 支配 (L_1, C_1),当且仅当 $L_1 \leqslant L_2$ 且 $C_1 \subseteq C_2$,记为 $(L_2, C_2)\,\mathrm{dom}\,(L_1, C_1)$。

简单安全条件　安全域 S_1 可以通过单向传输装置提交数据客体 O 到安全域 S_2,当且仅当 S_2 dom S_1 dom O 且 S_1 对数据客体 O 有自主控制权。

属性　安全域 S_1 可以跨域引用监视器发布数据 O 到安全域 S_2,当且仅当 S_1 dom S_2 dom O 且 S_1 对数据有自主控制权。

基本安全定理　设系统 Σ 的某一个初试安全状态为 σ_0,T 是状态转换集合。如果 T 的每一个元素都遵守简单安全条件和属性,那么对每一个 $i \geqslant 0$,状态 σ_i 都是安全的。

5　结语

本文针对目前 MLS 系统存在的问题,通过设计一个系统级的跨域引用监视器,实现以数据为中心的多级安全模型。利用该安全模型研发了基于密标和数字签名的跨域传输单向系统,该单向传输系统通过了安全保密评审和测试,并在不同密级的安全域之间部署使用,实现了信息从低密级网络流向高密级网络,也允许高密级网络把低密级数据发布给低密级网络,禁止高密级网络的高密级信息和无密级标记信息流向低密级网络,满足了 MLS 要求。下一步研究工作是在以数据为中心的多级安全模型的基础上,通过 Web 访问框架来支持以应用为中心的多级安全模型,并对其进行安全性分析。

参考文献:

[1] BELL D E, LAPADULA L J. Secure computer systems: unified exposition and multics interpretation [R]. Bedford: MITRE Corporation, 1976.

[2] BELL D E. Looking back at the Bell-La Padula model, VA 20191 [R]. Bedford: [s. n.], 2005.

[3] BELL D E. Looking back at the Bell-La Padula model[C]// ACSAC '05 Proceedings of the 21st Annual Computer Security Applications Conference. Washington, DC: IEEE Computer Society, 2005: 337 - 351.

[4] MULLER E, GRANT T, POLL E. Multilevel security[EB/OL]. [2010-12-10]. http://www.dodccrp.org/events/13th_iccrts_2008/CD/html/papers/124.pdf.

[5] Security target for LSPP, CAPP, and RBACPP compliance[R/OL]. [2012-11-10]. http://wenku.it168.com/d_000442844.shtml.

[6] LOSCOCCO P A, SMALLEY S D, MUCKELBAUER P A, *et al*. The inevitability of failure: the flawed assumption of security in modern computing environments[EB/OL]. [2012-10-10]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.76.6442.

[7] RUSHBY J. Design and verification of secure systems[C]// Proceedings of the 8th ACM Symposium on Operating System Principles. New York: ACM Press, 1981: 12 - 21.

[8] 卿斯汉. 高安全等级安全操作系统的隐蔽通道分析[J]. 软件学报, 2004, 15(12): 1837 - 1849.

[9] 一种无反馈单向传输的物理隔离方法: 中国, ZL200610140541.x [P]. 2006-10-17.

(下转第 742 页)

会稳定在平衡态 P_0^*；当 $I_0 \leqslant M_1$ 且 $R_0 \geqslant M_3$ 时，被感染节点不会全部消亡，只会稳定在另一个平衡态 P_1^*。仿真结果与理论分析结果一致。

同时，为了验证模型的有效性，本文通过与传统的 SIRS 计算机病毒模型[3-4] 进行比较。分别取参数 $b = 0.2$，$\beta = 0.2$，$\delta = 0.1$，$\gamma = 0.05$，$a = 0.5$，$\gamma = 0.05$，$a = 0.5$，$I_0 = 0.3$。

从图 6 可发现，改进模型较之相应传统模型，已感染节点比例下降速度明显加快，从而能使病毒传播更早得到有效控制。因此将阶段免疫接种加入到 SIRS 模型中，对计算机病毒研究具有现实意义。

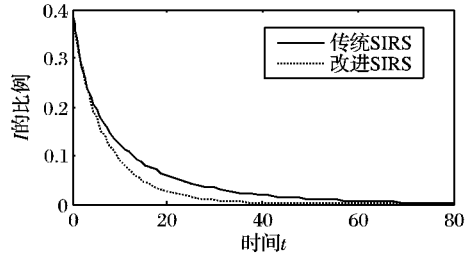

图 6 改进前后系统中已感染节点 I 所占比例的演化

另外为了研究设定感染阈值对病毒传播的影响，取参数值分别为 $S(0) = 0.7$，$I(0) = 0.21$，$b = 0.01$，$\beta = 0.5$，$\delta = 0.1$，$\gamma = 0.1$，$\varepsilon_0 = 0.05$，$I_0 = 0.2, 0.53, 1$。如图 7 所示，此时 $M_1 = 0.5238$。

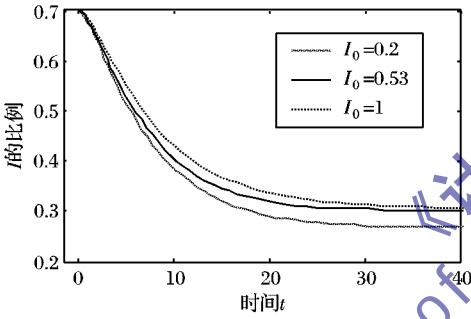

图 7 I_0 取不同值时系统中 I 的比例的变化对比

从图 7 可发现，当 $I_0 \leqslant M_1$ 且 $R_0 \geqslant M_3$ 时，提高免疫接种概率会使网络出现新的有毒平衡态，此平衡态下的感染节点比例相对采取措施前有所下降。同时控制感染阈值 I_0 可以使系统在两个平衡态之间转化，即当 $I_0 \geqslant M_1$ 时可能使系统由平衡态 P_1^* 转化为平衡态 P_0^*，此后随着感染阈值 I_0 的增大，系统趋于平衡的速度将减缓。

4 结语

本文考虑免疫接种的实际特点提出了一个改进的 SIRS 计算机病毒传播模型。该模型的理论分析和计算机仿真结果表明，系统随时间演化将可能出现 3 种平衡态，其动力学行为取决于感染阈值 I_0 的设定以及 R_0 的取值；1）该模型通过与传统 SIRS 模型比较，验证了阶段免疫接种对于病毒控制的有效性；2）与以往模型不同是该模型能更为客观的反映免疫接种策略在病毒传播中实施特点；3）在一定条件下，提高感染阈值 I_0 会减缓系统趋于平衡的速度。所得实验结论可以为病毒防控策略提供理论参考。

本文是旨在通过引入阶段免疫接种概率函数来研究阶段防控策略对病毒传播的影响。事实上已感染节点比例在达到感染阈值前后可能会有其他参数的变化[10]，导致两个阶段存在更大的差异。同时本文模型是建立在全连接网络上，然而真实的网络拓扑仍有待研究[8]，为此下一步的工作是将病毒阶段防控策略针对复杂网络做调整，比如对于大度节点有更高的概率免疫接种等，从而可以使模型得到更多有价值的结论。

参考文献：

[1] 张仁斌，李钢，侯整风. 计算机病毒与反病毒技术[M]. 北京：清华大学出版社，2006.

[2] KEPHART J O, WHITE S R. Directed graph epidemiological model of computer viruses[C]// Proceedings of 1991 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 1991: 343 - 359.

[3] 李玉辉. 具有双线性感染率和免疫接种 SIRS 模型的分析[J]. 北华大学学报：自然科学版，2011，12(2)：149 - 153.

[4] GAN C, YANG X, LIU W. Propagation of computer virus under human intervention: a dynamical model [EB/OL]. [2012-05-10]. http://www.hindawi.com/journals/ddns/2012/106950/.

[5] LI J, YANG Y, ZHOU Y. Global stability of an epidemic model with latent stage and vaccination [J]. Nonlinear Analysis: Real World Applications, 2011, 12(4): 2163 - 2173.

[6] 冯丽萍，王鸿斌，冯素琴. 改进的 SIR 计算机病毒传播模型[J]. 计算机应用，2011，31(7)：1891 - 1893.

[7] 张海峰，傅新楚. 含有免疫作用的 SIR 传染病模型在复杂网络上的动力学行为[J]. 上海大学学报：自然科学版，2007，13(2)：189 - 192.

[8] 夏承遗，刘忠信，陈增强，等. 复杂网络上带有直接免疫的 SIRS 类传染模型研究[J]. 控制与决策，2008，23(4)：468 - 472.

[9] MISHRA B K, PANDEY S K. Fuzzy epidemic model for the transmission of worms in computer network [J]. Nonlinear Analysis: Real World Applications, 2010, 11(5): 4335 - 4341.

[10] REN J, YANG X, ZHU Q, *et al*. A novel computer virus model and its dynamics [J]. Nonlinear Analysis: Real World Applications, 2012, 13(1): 376 - 384.

[11] LU Z, CHI X, CHEN L. The effect of constant and pulse vaccination on SIR epidemic model with horizontal and vertical transmission [J]. Mathematical and Computer Modelling, 2002, 36(9/10): 1039 - 1057.

[12] LUO Y, GAO S, YAN S. Pulse vaccination strategy in an epidemic model with two susceptible subclasses and time delay [J]. Applied Mathematics, 2011, 2(1): 57 - 63.

[13] ROBINSON R C. An introduction to dynamical systems: continuous and discrete [M]. London: Pearson Education, 2005.

（上接第 719 页）

[10] ANDERSON J P. Computer security technology planning study, ESDTR-73-51[R]. Bedford: Air Force Electronic Systems Division, 1972.

[11] KANG M H, MOSKOWITZ I S, LEE D C. A network version of the pump[C]// Proceedings of 1995 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 1995: 144 - 154.

[12] KANG M H, MOSKOWITZ I S, CHINCHECK S. The pump: a decade of covert fun[C]// Proceedings of the 21st Annual Computer Security Applications Conference. Piscataway, NJ: IEEE Press, 2005: 5 - 9.

[13] 信息技术产品安全测评报告[EB/OL]. [2010-12-10]. http://www.itsec.gov.cn/cpyzcgg/ggl26/.

[14] Developing a CC EAL7 multi-level security capability [EB/OL]. [2012-03-12]. http://www.commoncriteriaportal.org/iccc/7iccc/t1/t1210900.pdf.