时序 PLD 安全缺陷检测方法研究

陈志锋 李清宝 曾光裕
(解放军信息工程大学 郑州 450002)

摘 要 可编程逻辑器件(PLD)在电子设备中广泛应用,其安全缺陷检测已成为信息安全领域中一个富有挑战性的课题。通过分析 PLD 安全缺陷的存在形式,提出了基于状态转移图的安全缺陷检测方法。该方法统一了检测思路,采用了脱机式芯片逆向分析和在线式芯片逆向分析相结合的技术,适用于不同的 PLD 安全缺陷检测,同时根据存在形式提出了检测算法。最后通过模拟测试对该检测思路及算法的有效性进行了验证。

关键词 可编程逻辑器件,状态转移图,安全缺陷检测
中国法分类号 TP393.08 **文献标识码** A

Research on Sequential PLD Security Vulnerability Detection Method

CHEN Zhi-feng LI Qing-bao ZENG Guang-yu
(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Due to the wide application of PLD in the electronic devices, the vulnerability detection of PLD has become a challenging subject in the information security field. By analyzing the existence form of PLD security vulnerability, a security vulnerability detection method was proposed, based on state transition diagram. Using off-line reverse analysis and on-system reverse analysis technology, this method unifies the detection ideas, which is suitable for different PLD security vulnerability detection. Then the detection algorithms were proposed on the basis of the existence forms. Finally, the effectiveness of the detection ideas and algorithms were verified by simulation.

Keywords Programmable logic device, State transition diagram, Security vulnerability detection

1 引言

21世纪是信息的时代,现代信息产业的基础是电子设备,电子设备的核心因素是 IC(Integrated Circuit)芯片,IC 芯片自身的安全对信息系统的安全具有至关重要的作用[1]。其主要原因在于现代信息存储、传输和处理都需要依赖集成电路芯片,IC 本身的安全与否与被处理的信息及其安全息息相关。多年以来,黑客主要是通过软件的缺陷和漏洞或者后门来发动攻击,安全性防护和恶意代码的检测等技术研究也主要从软件层面上展开。CIH 病毒的发作让人们清醒地意识到芯片硬件攻击的存在。弗吉尼亚州立大学的陈志民和郭雪等人对于 FPGA 芯片中恶意电路的触发方式展开了深入研究,他们将 FPGA 芯片的热量通信与时序关系相结合,设计完成了一种硬件的恶意电路[2]。越来越多的事实表明,利用芯片本身的安全缺陷和漏洞实现攻击是可行的,其造成的危害可能更为严重。IC 的安全缺陷问题已成为当今信息安全领域研究的热点课题。

当前我国集成电路技术水平与发达国家相比还存在一定距离,长时期以来国内使用的大部分先进电子设备主要依赖进口,且这些设备中广泛使用了 PLD(Programmable Logic Device,可编程逻辑器件),如果这些器件中留有"攻击后门"、"恶意电路"或者"安全缺陷",将对我国的信息安全造成严重隐患。因此,及时发现芯片安全缺陷并采集相应防护措施很有必要。

自 2007 年开始,美国的部分信息安全研究人员已逐步转向对 IC 芯片内部的安全性漏洞和权限进行研究[3,4]。目前国际上对于芯片安全漏洞的研究正在蓬勃兴起[5,6]。当前常用的 IC 芯片安全缺陷检测方法主要有侵入式检测法、半侵入式检测法和非侵入式检测法[7-9]。侵入式和半侵入式安全缺陷检测方法受限于芯片拍摄图像的质量,对电路的检测还只停留在层次化电路图级别,这种研究随着芯片制造工艺的改进也正面临诸多局限。非侵入式检测弥补了侵入式和半侵入式的不足,特别适合发现芯片设计功能上的漏洞或缺陷。美国密歇根大学、瑞典 Chalmers 技术大学开发的硬件测试错误注入工具,为漏洞检测奠定了坚实的基础[10,11]。文献[12]提出利用电路的功耗分布图检测芯片安全缺陷。文献[13]提出基于指纹的旁路信号分析法,该方法通过芯片的指纹特征匹配发现芯片安全缺陷。这些方法都是利用旁路信号分析法进行安全缺陷的检测,不仅需要昂贵的设备,而且对于小型硬件木马或者安全缺陷,效果很微弱甚至无效。对于小型硬件木马

到稿日期:2011-06-27 返修日期:2011-09-28 本文受国家 863 目标导向项目(2009AA01Z434)资助。
陈志锋(1986—),男,硕士生,主要研究方向为信息安全,E-mail:xiaohouzi06@163.com;**李清宝**(1967—),男,博士,教授,主要研究方向为信息安全;**曾光裕**(1966—),女,硕士,副教授,主要研究方向为多媒体技术与信息安全。

或者安全缺陷，文献[14]提出一种新的逻辑测试方法来检测安全缺陷，该方法是基于触发芯片安全缺陷的稀有条件出现的次数实现的。文献[15]提出了内建测试技术，该技术是芯片的一个额外功能，通过该技术能够监测到芯片的恶意逻辑从而实现安全缺陷的检测。这些方法能够检测出 IC 中是否存在安全缺陷，但是无法准确定位安全缺陷和确定安全缺陷的存在形式。

因此针对检测方法的不足，本文以非侵入式安全缺陷检测技术为基础，结合脱机检测法和在线检测法，重点研究时序 PLD，提出基于状态转移图的安全缺陷检测方法。以下首先给出关于 PLD 安全缺陷及其检测涉及的基本定义，然后阐述 PLD 安全缺陷及其检测方法，最后通过实验论证检测方法的可行性和有效性。

2 基本定义

为了更好地论述 PLD 芯片安全缺陷检测方法，首先给出有关概念和问题的基本定义。

定义 1(PLD 安全缺陷) PLD 安全缺陷是指在可编程逻辑器件中，通过自身或者与其它芯片协同工作导致信息系统脆弱性的缺陷和不足。

定义 2(脱机式芯片逆向分析) 脱机式芯片逆向分析利用黑箱功能等价原理对逻辑器件进行逆向分析，将待解析的器件看成一只“黑箱”[16]，通过施加不同组合、不同序列的激励，在输出端采集其对应输出，运用逻辑综合的方法推导出引脚间的逻辑功能。

定义 3(在线式芯片逆向分析) 在线式逆向分析法是利用数据(波形)采集设备采集芯片在系统工作时的波形数据，通过对波形数据的分析得到芯片正常工作时的逻辑功能，其又称为在线式逻辑时序模拟法。

定义 4(功能全集) 功能全集是指利用脱机式芯片逆向分析技术采集芯片数据，通过数据分析得到芯片的全部逻辑功能组成的集合，这里定义为 A，且 $A\neq\phi$。

定义 5(工作集) 工作集是指利用在线式芯片逆向分析技术依托在线采集设备采集芯片工作时的波形数据，分析数据得到的逻辑功能组成的集合，这里定义为 B，且 $B\neq\phi$，$B\subseteq A$。

定义 6(可疑状态集) 可疑状态集是指功能全集与工作集的差集，这里定义为 C，且 $C=A-B$。

定义 7(安全缺陷状态集) 安全缺陷状态集是指经过安全缺陷检测技术检测后，被标识为安全缺陷的状态集合，这里定义为 D，且 $D\subseteq C$。

定义 8(状态转移图) 本文的状态转移图是基于 Mealy 自动机的，通过分析采集数据提取状态、输入输出关系绘制而成，定义为 $G=(S,E,L)$，其中 S 表示各个顶点状态，E 表示各个状态之间的转移关系，L 表示转移关系对应的输入输出。

定义 9(强连通分量[17]) 在图 G 中，若任意两个顶点 si 和 sj 间都存在从 si 到 sj 的路径及一条从 sj 到 si 的路径，则称 G 是强连通。G 的极大强连通子图，称为 G 的强连通分量。

3 PLD 安全缺陷及其检测方法

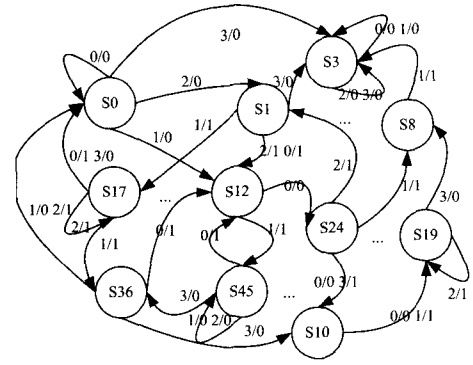
3.1 PLD 安全缺陷存在形式

有限状态机是对时序逻辑电路最重要的抽象表现形式，状态转移图是描述有限状态机行为的方法之一。本文根据定义 8 绘制对应的状态转移图描述时序 PLD 逻辑功能。据目前研究，时序 PLD 安全缺陷主要表现为孤立状态(或者孤立状态环)和冗余功能两种存在形式。

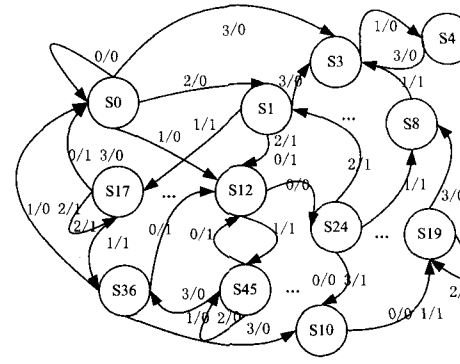
(1)孤立状态(环)

为了讨论方便，本文将孤立状态、孤立状态环统一称为孤立状态，详细定义见定义 10。

定义 10(孤立状态) 本文定义的孤立状态包含两种情况，一种指的是安全缺陷状态集 D 中有且仅有一个元素，并且不存在从集合 D 到集合 B 中的边，即纯粹的孤立状态，如图 1(a)所示的状态 $S3$；另一种是指的是若干个状态形成一个环，但是从某一个状态 S 进入该环后，不存在从该环中所有状态到 S 的路径，并且安全缺陷状态集 D 的元素个数大于 1，即孤立状态环，如图 1(b)所示的状态 $S3$，$S4$ 组成的环。



(a) 孤立状态



(b) 孤立状态环

图 1 孤立状态示意图

(2)冗余功能

硬件冗余有两方面的含义：进行故障屏蔽和埋置漏洞后门。为了提高硬件系统的可靠性，结构冗余是一项经常被采用的技术。本文研究的逻辑器件的冗余功能主要是指可被恶意利用的安全缺陷。

冗余功能是指芯片在完成正常功能后，还存在尚未执行的不明逻辑功能，虽然不明冗余功能可能不会影响芯片的正常功能，但它增加了潜在的攻击隐患。如图 2 所示，虚框中的状态即为某一芯片的冗余功能状态，恶意攻击者可以利用这些冗余功能，在冗余状态下设计实现恶意攻击，譬如系统死

机、信息泄露等；与孤立状态安全缺陷不同的是存在冗余功能状态到其他状态的路径，为此，这种安全缺陷可以通过某种手段（譬如无线、网路数据包等）恢复系统进入正常工作状态。

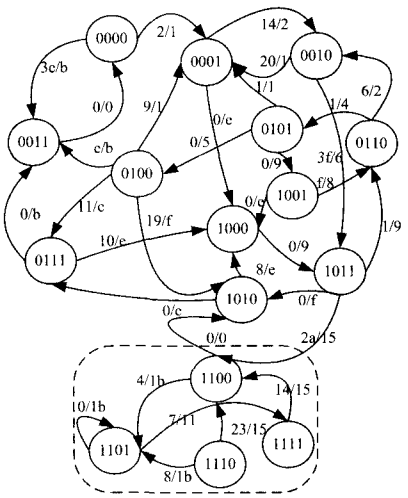


图 2　冗余功能示意图

3.2　PLD 安全缺陷检测方法

根据 PLD 芯片自身的硬件特性，PLD 安全缺陷检测方法不同于软件漏洞安全缺陷检测，其检测必须结合硬件环境。为此，本文提出一种基于状态转移图的安全缺陷检测方法。该方法把脱机式和在线式逆向分析技术相结合，通过分析功能全集和工作集确定可疑状态集，并结合芯片工作环境最终确定安全缺陷状态集。该方法利用可视化技术将 PLD 逻辑功能转换成可视的状态转移图，结合安全缺陷的存在形式、硬件环境和图论理论进行安全缺陷检测。其检测方法工作流程如图 3 所示。

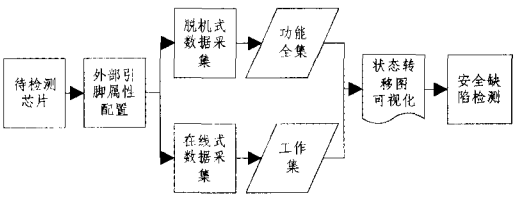


图 3　PLD 安全缺陷检测方法流程

3.2.1　孤立状态安全缺陷检测

定理 1　有且仅有一个强连通分量的状态转移图对应的 PLD 不含有孤立状态安全缺陷。

证明（反证法）：假设只有一个强连通分量的状态转移图包含孤立状态安全缺陷。根据定义 10，孤立状态安全缺陷不存在从孤立状态到其他状态的转移关系，即从孤立状态到其他状态不存在出边。根据定义 9，该状态转移图为非强连通图，包含的强连通分量个数大于 1，这与假设只有一个强连通分量矛盾。因此，假设不成立，定理得证。

根据定理 1，孤立状态安全缺陷检测主要是要查找芯片中从一个状态不可逆到另一个状态或者存在多个强连通分量的情况。首先获取芯片功能全集，绘制对应的状态转移图，分析状态转移图查找强连通分量个数，然后依据强连通分量个数进行进一步的分析。

根据该思想，在图 3 所示的检测方法流程的指导下，检测算法实现流程，如图 4 所示。

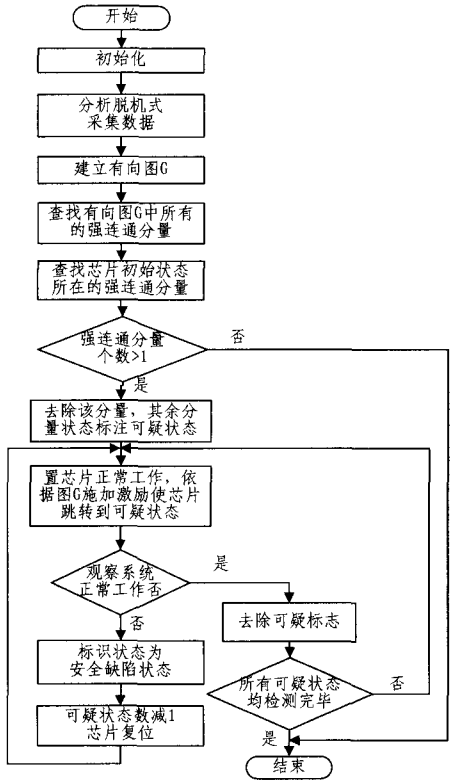


图 4　孤立状态安全缺陷检测算法流程图

3.2.2　冗余功能安全缺陷检测

冗余功能安全缺陷检测借鉴集合论思想实现。

定理 2　当且仅当 $C\neq\phi$，冗余功能安全缺陷状态才存在。

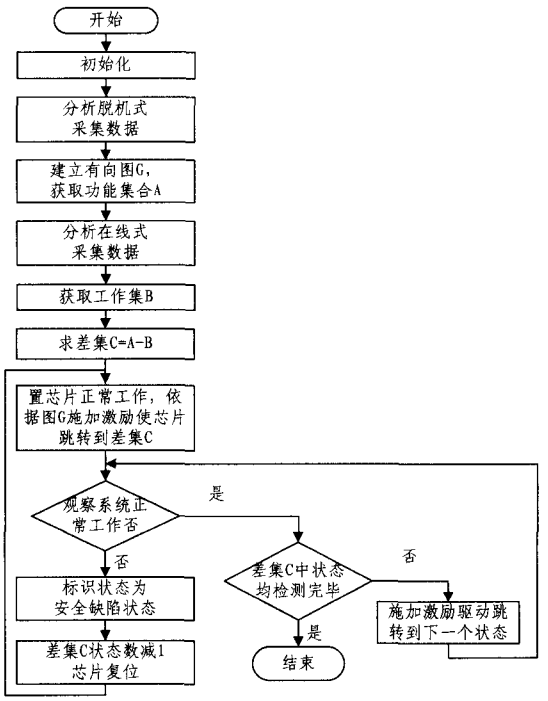


图 5　冗余功能安全缺陷检测算法流程图

证明（必要性）：假设可疑状态集 $C=\phi$，根据定义 6，则 $A=B$，即功能全集等价于工作集。由于工作集是芯片正常工作时对采集的芯片波形数据进行分析得到的集合，而功能全集包含了芯片的全部功能状态，因此不存在多余的状态，亦即

不存在冗余功能安全缺陷。

(充分性)假设存在冗余功能安全缺陷状态,即 $D\neq\phi$,根据定义 7,$D\subseteq C$,因此 $C\neq\phi$。证毕。

根据定理 2,冗余功能安全缺陷检测的关键是要获取到可疑状态集 C。首先通过脱机式芯片逆向分析获取芯片逻辑功能全集 A,然后通过在线式逆向分析技术获取芯片工作集 B,A 与 B 的差集 C 即为可疑状态集(冗余功能集)。同样置芯片于工作环境施加激励驱动芯片进入冗余功能集,观察芯片所在系统的状态,若出现异常,则存在冗余功能安全缺陷。冗余功能安全缺陷检测算法如图 5 所示。

4 实验与分析

根据安全缺陷检测算法及检测流程,本文实现了基于状态转移图的 PLD 安全缺陷检测系统。系统可完成 PLD 的数据采集和分析结合可视化技术实现安全缺陷的检测。为了能清晰地展示检测过程,实验先以 51 开发板中一个简单的案例为例,该开发板模拟仿真了一个简易的交通灯系统,并且在该系统中设计了安全缺陷。本实验通过检测该开发板上是否存在安全缺陷来验证检测算法的可行性和正确性。检测对象为开发板上有若干个 PLD 芯片,检测软件放置在配置为 AMD Athlon 64 X2 Dual Core Processor 4200+ 2.21Ghz、1G 主存的 PC 机上。经过相应的检测步骤,最终在 Lattice Gal 22V10D 芯片上定位到安全缺陷,该安全缺陷属于冗余功能安全缺陷。检测过程如下,经过脱机式数据采集,得到的功能全集状态转移图包含 8 个状态,进行孤立状态安全缺陷分析后发现,该状态转移图中只包含 1 个强连通分量(若有若干个强连通分量,则有不同种颜色),如图 6 所示,因此该芯片不存在孤立状态安全缺陷;接着进行在线式数据采集,通过冗余功能安全缺陷分析后发现,芯片工作时只出现 4 个状态 0000、0001、0010、0011(绿色表示),其他 4 个状态 0100、0101、0110、0111(紫色表示)并未出现,如图 7 所示。到此我们初步怀疑这 4 个状态,然后置芯片于 51 开发板工作环境,通过键盘输入施加特定激励,驱动芯片进入状态 0100,观察开发板工作情况,此时出现交通灯停止工作状况,可见芯片进入状态 0100 后系统出现异常,为此可以判定状态 0100 为安全缺陷状态。类似,可以判定其他状态。此外,实验还对其他若干芯片进行了安全缺陷检测,在实验室自主开发的安全缺陷模拟仿真设备上模拟多种 PLD 安全缺陷,并利用本文提出的检测方法进行实验,检测结果如表 1 所列。其主要列出了 4 种不同规模芯片的安全缺陷检测过程,其中两个芯片含有安全缺陷,对应于本文总结的两类存在形式的安全缺陷,并且这两个安全缺陷实现了不同的安全攻击,另外两个芯片则不含安全缺陷。实验证明,安全缺陷检测方法是可行和有效的;将其应用于某 863 项目中,取得了较好的实际效果。

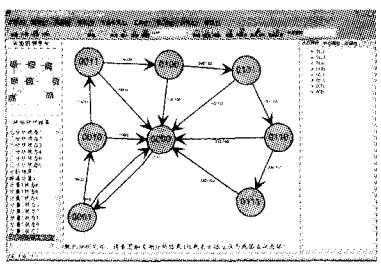


图 6 经过孤立状态安全缺陷检测后的状态转移图

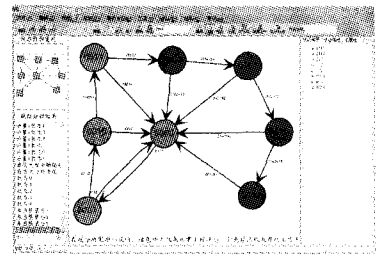


图 7 结合在线式采集数据分析后的状态转移图

表 1 安全缺陷检测一览表

芯片	脱机采集状态数	在线采集状态数	可疑状态数	检测出的安全缺陷类型	表现
EPM7032	1024	1021	3	孤立状态	系统死机
EP610	485	430	55	冗余功能	功能紊乱
GAL 22V10	64	64	0	无	正常
GAL 20V8	96	93	3	无(故障屏蔽)	正常

结束语 随着集成电路的发展,PLD 的规模不断扩展,其结构也日益复杂。这给脱机式逆向分析和在线式逆向分析带来了巨大的挑战,主要表现在测试激励集规模随芯片的输入输出规模以指数级增长以及在线式采集设备的存储深度受限,同时也提高了安全缺陷的检测难度。在有限的存储条件下,如何设计合理的状态图结构用于数据采集以及安全缺陷检测,如何解决在线采集数据的完备性问题均是下一步需要研究的重点。此外,PLD 安全缺陷的存在形式、触发机制趋于多样化等给检测也带来了更大的难度,深入研究 PLD 安全缺陷的存在形式、触发机制等也是下一步的重点。

参 考 文 献

[1] 王阳. 构建信息化社会的物质基础[EB/OL]. http://www.paper.edu.com

[2] Chen Zhi-min, Guo Xu, Nagesh R. Hardware Trojan Designs on BASYS FPGA Board[EB/OL]. http://filebox.vt.edu/users/xuguo/homepage/pu-blications/csaw08.pdf, 2008-09-19

[3] Chakraborty R S, Paul S, Bhunia S. On-demand transparency for improving hardware Trojan detectability [C]// Proc of IEEE International Workshop on Hardware-Oriented Security and Trust. Wuhan, China, 2008: 48-50

[4] Stefan D, Mitchell C, Almenar C G. Trojan Attacks for Compromising Cryptographic Security in FPGA Encryption Systems [EB/OL]. http://199.98.20.129/~stefan/projects/csaw08/csaw08_cooper_submission/cooper_csaw08.pdf, 2008-09-27

[5] Wolff F, Papachristou C, Bhunia S, et al. Towards trojan-free trusted ics: problem analysis and detection scheme[C]// Proc of Design Automation and Test in Europe. 2008: 1362-1365

[6] Adamov A, Saprykin A, Melnik D, et al. The Problem of Hardware Trojans Detection in System-on-Chip[C]// Proc of CAD Systems in Microelectronics. Polyana-Svalyava UKRAINE, 2009: 178-179

[7] Marsh C, Kean T. A Security Tagging Scheme for Application Specific Intellecture Property Cores [EB/OL]. http://www.carolmarsh.co.uk/resources/Tagging_ESS_11_10_06.pdf, 2008-10-11

[8] Skorobogatov S, Anderson R. Opticail Fault Induction Attacks, Cryptographic[C]// Proc of Hardware and Embedded System Workshop. LNCS, Springer-Verlag, 2002: 2532: 2-12

(下转第 79 页)

的参考。

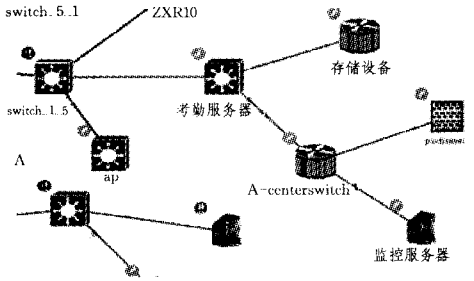


图 6 上下班场景业务逻辑图

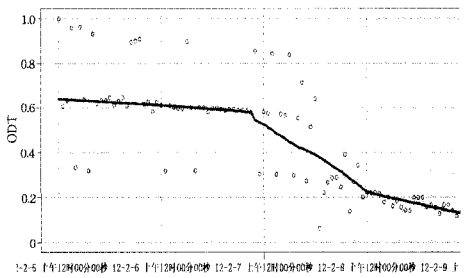


图 7 考勤业务的总体信任度变化趋势图

结束语 本文根据 ITIL 平台特点，提出了一种根据动态管理模型理论计算业务信任值的方法，并将信任值的变化用于监控系统内部的安全环境。在此基础上，结合现有的 ITIL 平台开发环境，建立了基于 ITIL 平台的动态访问控制模型，实现了针对业务的行为验证。该模型以 ITIL 标准中安全服务级别协议(SLA)和安全事件管理规范，为上下文环境的信任相关因素，动态地计算和变更计算资源的信任值，以期减少由于设备安全动态变化造成的网络服务可信性损失。下一步工作将集中探讨 ITIL 下信任数据存储、规模与效率等问题。

参 考 文 献

[1] Clifford D, van Bon J. Implementing ISO/IEC 20000 Certification: The Roadmap. ITSM Library[S]. Van Haren Publishing, 2008

[2] 张明德. 身份认证可信度研究[J]. 计算机科学, 2011, 38(11): 43-47

[3] Blaze M, Feigenbaum J, Lacy J. Decentraliezed trust management[C]//Bale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Washington: IEEE Computer Society Press, 1996: 164-173

[4] Policy Maker[EB/OL]. www. polimap. com/

[5] Keynote [EB/OL]. www. keynotesecurity. com/

[6] Marsh S P. Formalizing trust as a computational comcept [D]. Stirling: University of Stirling, 1994, http://www. nr. no/~abile/Papers/TR133. pdf

[7] Almenárez F. PTM: A pervasive trust management model for dynamic open environments[C]//Workshop on Pervasive. 2004

[8] Nefti S. A fuzzy trust model for e-commerce[C]//E-Commerce Technology. 2005

[9] Sepandar D K. The EigenTrust algorithm for reputation management in P2P networks[C]//Proceeding WWW '03 Proceedings of the 12th international conference on World Wide Web

[10] 李小勇. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6): 1510-1521

[11] 赛迪网. TSM: 中国银行广东省分行 IT 服务管理案例[EB/OL]. http://industry. eeidnet. eom/art/19/20040402/99965_1. html, 2004-04

[12] 王华. 上海西门子移动通信有限公司实施 IT 服务管理的策略研究[D]. 上海: 上海交通大学, 2008

[13] 张孜. 基于 ITIL 理念的交通信息设施运维管理系统设计与实践[J]. 交通运输系统工程与信息, 2011(4): 41-45

[14] 刘海峰. 基于 ITIL 体系的安全服务级别管理研究[J]. 计算机工程与设计, 2007(4): 780-784

[15] ca 公司. eTrust TM Security Management[EB/OL]. http://www3. ca. com/solutions/Solution. aspx? ID=271

[16] 桂小林. 网格技术导论[M]. 北京: 北京邮电大学出版社

[17] Peng N, Yun C, Reeves D S. Analyzing Intensive Intrusion Alerts via Correlation[C]// Proc of the 5th International Symposium on Recent Advance in Intrusion Detection. Zurich, Switzerland, 2002

[18] Savla S, chakravarthy S. An efficient single pass approach to frequent episode discovery in sequence data[C]//IET 4th International Conference. 2008

[19] Fuller R, Majlender P. An analytic approach for obtaining maximal entropy OWA operator weights[J]. Fuzzy Sets and Systems, 2001(1): 53-57

[20] 石贵民, 林宏基. 基于旁路的网络流量监控模式[J]. 重庆理工大学学报: 自然科学版, 2011, 25(9): 63-69

(上接第 56 页)

[9] Golden C, Cartridge T. Computer Chip Usage and the Impact on the After market[J]. Static Control Components, 2002: 36-46

[10] Chang K-H, Markov I L, Bertacco V. Fixing Design Errors with Counter-examples and Resynthesis[J]. IEEE Trans. on Computer-Aided Design, 2008, 27(1): 184-188

[11] King S T, Tucek J, Cozzie A, et al. Designing and implementing malicious hardware [EB/OL]. http://www. usenix. org/event/leet08/tech/full_papers/king /king. pdf, 2009-04-11

[12] Banga M, Chandrasekhar M, Lei Fang, et al. Guided test generation for isolation and detection of embedded Trojans[C]//Proc of the 18th ACM Great Lakes Symposium on VLSI. 2008: 363-366

[13] Agarwal D, Baktir S, Karakoyunlu D, et al. Trojan detection using IC fingerprinting[C]//Proc of IEEE Symp on Security and Privacy. 2007: 20-23

[14] Chakraborty R S, Wolf F, Papachristou C, et al. Towards trojan-free trusted ics: Problem analysis and detection scheme[C]//Proc of design, automation and test conference. 2008: 1362-1365

[15] Sanno B. Detecting Hardware Trojans[EB/OL]. http://www. crypto. rub. de/imperia/md/content/seminare/itsss09/benjamin_sanno. semembsec_termpaper_20090723_final. pdf. 2009-07-22

[16] Friedenberg J. Mind as a Black Box[M]. Sage Publications, 2006: 85-88

[17] 唐策善, 李龙澎, 黄刘生. 数据结构—用 C 语言描述[M]. 北京: 高等教育出版社, 2006: 125