面向互联网电子政务的定制数据安全交换技术研究综述*

孙 奕[1,2,3], 毛 琨[2], 陈性元[2], 杜学绘[2]
(1. 北京交通大学 计算机与信息技术学院, 北京 100044; 2. 解放军信息工程大学, 郑州 450004; 3. 数学工程与先进计算国家重点实验室, 郑州 450004)

摘 要: 为了解决互联网电子政务信息的安全共享与交换问题,提出一种交换策略可定制、交换数据可信、交换行为可控的定制数据安全交换模式。重点分析了定制数据安全交换模式下存在的安全威胁;针对安全威胁提出了相应的解决方法,并总结分析了所涉及关键技术的研究现状与不足之处;最后指出了定制数据安全交换未来的研究热点及发展前景。

关键词: 定制交换; 基于属性的加密体质; 专用交换进程建模与度量
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2014)04-0965-05
doi:10.3969/j.issn.1001-3695.2014.04.002

Survey of customized data security exchange technology for e-government

SUN Yi[1,2,3], MAO Kun[2], CHEN Xing-yuan[2], DU Xue-hui[2]
(1. *School of Computer & Information Technology, Beijing Jiaotong University, Beijing* 100044, *China*; 2. *PLA Information Engineering University, Zhengzhou* 450004, *China*; 3. *State Key Laboratory of Mathematical Engineering & Advanced Computing, Zhengzhou* 450004, *China*)

Abstract: In order to solve the problems of information sharing and exchanging for e-government, this paper proposed a customized data security exchange mode which could customize and control the exchange strategy, the exchange data and the exchange behavior. Then this paper analysed the security threat of the customized data security exchange mode and proposed the corresponding solutions. Furthermore it summarized and analyzed the current status and the deficiency of the key technologies of the currently customized data security exchange. At the end it discussed the future research directions of customized data security exchange technology.

Key words: customized secure exchange; ABE(attribute-based encryption); private exchange process modeling and measurement

国民经济和社会发展的“十二五”规划建议中,明确提出“以信息共享、互连互通为重点,大力推进国家电子政务网络建设,整合提升政府公关服务和管理能力。”一方面,电子政务信息共享能够提高政府的行政执行力、政策实施的准确性和有效性,改善政府的管理和服务;另一方面,电子政务信息在共享与交换的过程中也带来了敏感信息泄露、恶意代码传播等安全问题。因此研究互联网电子政务信息的安全共享与交换问题具有重要意义。为了解决互联网电子政务信息安全共享与交换问题,本文提出一种交换策略可定制、交换数据可信、交换行为可控的定制数据安全交换模式。

1 定制数据安全交换的相关概念

1.1 内部数据处理区域和公开数据处理区域

根据基于互联网电子政务信息安全实施指南 GB/Z 24294[1] 中分域控制的要求,互联网电子政务安全域划分为内部数据处理区域、公开数据处理区域。其中公开数据处理区域用来承载处理公开信息的电子政务应用系统及其数据库,处理对公众和企业开放的服务,如政策发布、政府网站或便民服务等,这些都是提供给公众访问的公开数据。内部数据处理区域用来承载处理内部信息的电子政务应用系统及其数据库,处理政府内部和部门之间的业务,这些是仅允许系统内部人员访问的内部数据。

1.2 定制数据安全交换模式及交换步骤

定制数据安全交换模式是指基于定制的交换策略对特定格式的、静态的异构数据进行统一适配、转换、过滤、传输与加载的处理过程。这种模式的特点是一般面向特定的交换对象,对信息安全交换行为的控制能力较强,主要适合于交换信息固定、交换行为可预定义的跨域安全交换,如文件交换、数据库同步等。定制交换模式如图 1 所示,具体交换步骤如下:

a)交换数据生成过程。内部数据处理区中的交换适配区根据定制的交换策略从政务办公系统中提取交换信息,将交换信息转换为统一的格式并进行加密、签名处理,然后放入交换

收稿日期: 2013-07-26; **修回日期**: 2013-09-18 **基金项目**: 国家“973”计划资助项目(2011CB311801);国家“863”计划资助项目(2012AA012704);河南省科技创新人才计划资助项目(114200510001)

作者简介:孙奕(1979-),女,河南郑州人,讲师,博士研究生,主要研究方向为网络安全(11112072@bjtu.edu.cn); 毛琨(1986-),男,硕士,主要研究方向为信息安全;陈性元(1963-),男,教授,博导,博士,主要研究方向为信息安全、分布式操作系统;杜学绘(1968-),女,教授,硕导,主要研究方向为信息安全、算法分析.

缓冲区。

b)交换数据传递过程。对发送节点上的专用交换进程完整性进行验证,验证通过后闭合专用进程控制点,启动内部处理区和交换主节点的专用进程将信息从内部处理区的缓冲区交换到主节点的缓冲区中,任务完成后打开专用进程控制点。

c) 交换数据过滤过程。首先依据对交换数据源认证的结果和交换策略对缓冲区中的交换信息进行过滤,然后依据定制的交换任务将过滤后的信息在访问控制策略控制下调度到相应的接收缓冲区中。

d) 交换数据加载过程。对接收节点上的专用交换进程完整性进行验证,验证通过后闭合专用进程控制点,启动专用进程将信息交换到公开数据处理区的交换缓冲区中,经过适配区的转换发送给公共服务系统。

整个交换过程均在交换行为的管控下进行,当出现异常行为时立即终止信息交换。

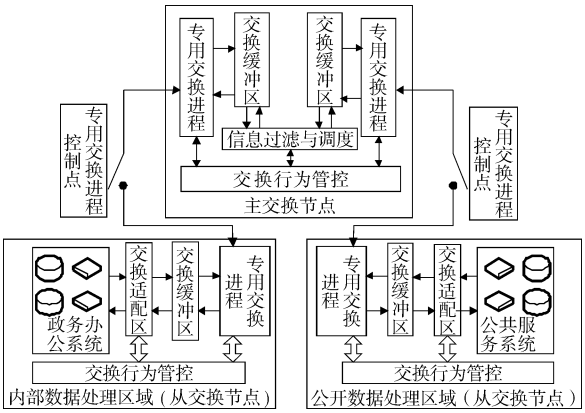

图1 定制交换模式

2 定制数据安全交换安全威胁分析

面向互联网电子政务的定制数据安全交换模式的风险主要来自于木马攻击、非法进程接入、信息窜改、信息夹带和非授权访问等造成的敏感信息泄露问题。基于以上的交换模式,数据安全交换面临的安全威胁主要有以下三个方面:

a)交换数据源面临的安全威胁。交换数据源是指交换数据产生的源头,交换数据源面临的安全威胁主要表现在以下三个方面:(a)攻击者利用恶意代码直接窃取交换数据,破坏交换数据保密性;(b)非授权访问造成的信息泄露,未授权的交换进程有意或无意获得交换数据;(c)攻击者对交换数据的非法窜改,破坏交换数据完整性。

b)交换数据生成过程和加载过程面临的安全威胁。交换数据生成过程和交换数据加载过程主要运行在需要交换数据的从节点上,完成对数据源的提取和目标数据源的加载工作。在交换从节点上攻击者通过执行来自内部的或外部的恶意代码,对交换进程进行破坏、伪装或劫持,使得交换进程无法按照预期的目标正确执行,间接造成信息的窜改、泄露和非授权访问等安全威胁。

c)交换数据传递过程中面临的安全威胁。主交换节点可以是一个或多个,当主交换节点是一个时,数据交换是一种集中式的定制数据安全交换模式,当主交换节点为多个时,数据交换是一种分布式的定制数据安全交换模式。正常情况下,主交换节点和从交换节点通过专用交换进程完成交换数据的传递。此时,攻击者可以利用内部数据处理区域上的恶意代码(如木马)作为独立的进程,读取敏感数据,绕过专用交换进程直接向公开数据处理区域上的木马发起连接,通过木马将敏感信息泄露到公开数据处理区域上。恶意代码之所以能够建立起连接,是因为缺乏对数据安全交换网络的管理,缺少对数据安全交换网络连接的控制,导致木马程序可以作为独立的进程连接交换网络。

3 定制数据安全交换关键技术研究

根据定制数据安全交换的特点以及安全威胁分析,本文提出从保证交换数据源安全和交换行为可信两个方面来解决定制数据安全交换问题。一方面,交换数据源安全即要保证交换数据保密性、完整性、可用性、可控性和抗抵赖性,可以应用密码技术来解决,但是随着云计算、物联网等新技术的发展,传统的密码技术在使用上存在缺陷,因此本文研究基于属性加密的方法来解决交换数据安全性问题;另一方面,如图1所示的定制数据安全交换模式下,交换任务、交换步骤以及交换数据是可以定制的,因此可以研发专用的交换进程,并制定相应的准则来规范和评估专用交换进程行为。本文研究专用交换进程行为建模与度量方法来解决交换行为可信的问题,为交换行为监管提供依据。

3.1 基于属性加密的数据安全交换方法研究

当交换信息含有敏感数据、交换代理不可信或交换信息存储介质不可信(如云存储系统[2])时,要防止敏感信息的泄露及非授权访问,因此需要对交换数据实施保密性和访问控制措施。

为了实现交换数据的保密性和细粒度访问控制,传统的基于PKI的方案[3,4]要么引发很高的密钥管理负担,要么需要使用不同用户的密钥加密一个文件的多个副本。为了提高以上方法的可扩展性,需要一个具有一对多的加密方法。

2005年,Sahai等人[5]首次提出了基于属性的加密机制(ABE),ABE是一种把属性和身份相结合的密码学体制,是一种one-to-many的加密体质。在此体制中,身份被描述成一个特征串,基于属性的加密体制可以分为两类,一类是密钥策略的基于属性加密体制(KP-ABE)[6],另一类是密文策略的基于属性加密体制(CP-ABE)[7~9]。当密钥和访问策略相结合时就称为KP-ABE;当密文和访问策略相结合而密钥对应一个属性集合时就称为CP-ABE,解密当且仅当属性集合能够满足此访问策略。

Goyal等人[6]提出的KP-ABE方案首次解决了在互联网上敏感数据如何基于加密的方法实现细粒度访问控制。该方案基于属性对数据进行加密,密钥与访问策略绑定,只有拥有适当密钥的一个用户或一组用户才能解密数据,通过对数据的细粒度访问完成敏感信息在不同用户之间的安全共享与交换。该方案不仅实现对信息的细粒度访问,而且大大提高了加密和密钥管理的效率,为实现在不完全可信的环境下敏感信息的安全共享与交换提供了一种新思路。从此在这方面展开了许多研究,例如,文献[10~13]给出了在对数据外包服务(如云服务)下,基于ABE的信息安全共享方案;文献[14~17]给出了电子医疗记录系统中基于ABE的电子医疗记录信息的安全共享问题。

但是以上方案都存在一个共同的缺点,即系统中只有一个可信的授权机构(TA),这样不仅会产生负载瓶颈,也会由于TA能够访问所有的加密文件从而产生密钥泄露和隐私泄露的

问题,而且委托一个授权结构管理所有的属性(包括所有用户的属性或角色、产生密钥等)也是不现实的。为了解决这些问题,Chase[18]提出了多授权的基于属性的加密方案(MA-ABE),该方案的特点是有多个授权机构,多个授权机构通过一个中心授权机构(CA)可以实现非交互授权,随后 Chase 等人[19]又进一步将该方案改进为一个无 CA 的多授权的基于属性的加密方案(CC MA-ABE)。后来 Lewko 等人[20]在 2011 年的欧密会上提出一种无 CA 的多授权的分布式的基于属性的加密方案(LW-ABE),虽然 LW-ABE 比 CC MA-ABE 可以更好地表达策略,但是这些方案都是将访问策略与密钥绑定,当权限撤销时密钥撤销的通信负荷会很重。

这正是基于 ABE 解决信息安全共享与交换方案中面临的另一个重要挑战。为了支持策略的动态更新,方案中需要具有高效的、即时的权限撤销机制。传统的方法是授权机构通过定期的广播密钥来频繁地更新未撤销权限的用户,这种方法不能获得前向/后向安全并且效率也不高。

Yu 等人[13]提出 YWRL ABE 方案,一个数据的拥有者可以对数据进行加密并通过将包括基于属性的访问策略的密钥分发给授权用户使多个用户共享数据;他们也提出数据的拥有者可以通过将受影响的密文和密钥的更新授权给第三方服务器(如云服务)来提高撤销用户权限的效率,密钥的更新操作可以通过聚合操作来提高效率,降低负载;然而 YWRL 方案中仍然只有一个 TA。Li 等人[21]结合 CC MA-ABE 与 YWRL ABE 各自的优势,使信息共享系统中能够支持高效的、即时的权限撤销机制。

综上所述,对于基于 ABE 的数据安全交换方案的研究方向是在敏感信息和访问权限安全的前提下,尽可能地提高系统效率。此外,随着 ABE 机制的深入研究,对基于 ABE 的数据安全交换方案的研究也必会产生深远的影响。值得关注的是,目前还没有用于互联网电子政务系统中基于 ABE 的电子政务资源信息的安全共享与交换方案,更加没有考虑政务系统中基于工作流语义的数据安全交换问题。

3.2　专用交换进程行为建模与度量方法研究

3.2.1　进程行为建模相关研究

1996 年,Forrest 等人[22]通过实验证实,对于正常运行的进程,其行为序列是稳定的、呈规律性的,而当进程被攻击后,行为序列中会出现一些不常见的短序列。这项发现可以用于区别进程的正常行为与异常行为。基于此发现,Forrest 等人首先提出 TIDE 方法列举现在训练数据中所有唯一的、固定长度为 K 的短序列来构造进程正常行为轮廓的数据库。文献[23]论证了局部区域的不匹配数目有时也能够较好地表征异常行为,进而提出了改进的 STIDE 方法。Wagner 等人[24]考虑了进程行为序列的出现概率,提出了带频率门限的 STIDE 方法,即 t-STIDE。

在上述基于固定长度短序列的建模方法基础上,Debar 等人[25]首次提出采用变长序列作为行为模式,Eskin 等人[26]提出了基于变长时间窗的方法提取变长序列,以及 Wespi 等人[27]引入寻找 DNA 序列中不定长模式的思想,采用 Teiresias 算法发现进程行为的变长模式,变长模式兼顾长序列带来的精度以及短序列带来的计算有效性。

基于进程当前行为只与前一时刻行为有关的假设,文献[28]引入马尔可夫链,从状态转移的角度来描述进程行为;Lee 等人[29]将数据挖掘引入进程行为评估模型,利用改进的 RIPPER 算法挖掘进程行为的规则建立进程行为评估模型,用改进的 Apriori 算法从训练序列中挖掘模式,建立模型来评估进程。后来文献[30]采用最小熵长度描述进程轨迹中的用户行为不变性,并结合程序行为不变性对系统调用异常进行检测。之后又陆续衍生出其他建模方法,如 AADL 进程子集行为语义研究[31]、基于系统调用和进程代数 CCS 的行为建模方法[32]、基于非均匀半马尔可夫模型的行为迁移过程研究[33]等。

3.2.2　进程可信度量方法相关研究

交换网络连接首先对交换专用进程进行可信度量,然后根据度量结果进行裁决,最后根据裁决结果控制是否允许交换进程连接到交换网络。其重点在于对进程的可信度量,进程的可信取决于其执行环境可信和运行时可信。下面对进程执行环境可信度量和运行时可信度量的相关研究现状进行分析。

1)进程执行环境的可信度量方法

专用交换进程的执行环境主要依赖于软件包以及系统内核,本文将软件包与系统内核统称为专用交换进程的执行环境。执行环境如果不可信,则会影响到专用交换进程的运行,就有可能受到不可信环境的干扰或攻击。一旦潜伏在执行环境中的安全漏洞被攻击者利用,数据安全交换将面临被破坏的危险。因此,必须构建可信应用环境才能为数据安全交换提供保障[34]。

文献[35]为保证进程执行环境的安全,提出对进程所依赖的文件完整性进行度量的方法。进程 p 相关的文件有 f_1, f_k,…,f_n,首先计算进程 p 的所有相关文件的摘要值 $H(f_1)$, $H(f_k)$,…,$H(f_n)$,进行简单连接,再次计算摘要值 $H(H(f_1)\mid H(f_k)\mid\cdots\mid H(f_n))$作为执行环境度量的基准。

文献[36]在其基础上,基于无干扰理论对该方法进行了分析,证明了该执行环境的可信性与基于可信根的无干扰可信模型等价。然而该方法只考虑到了可执行程序与软件包之间的直接依赖关系,而忽略了软件包之间存在着依赖关系,即进程对软件包的间接依赖关系。该方法只能确保可执行程序所调用的软件包是完整的、未遭到破坏的,而可执行程序所调用的软件包可能依旧依赖于其他的软件包,而该软件包的完整性可能是未经过完整性度量的。若该软件包遭到窜改,则会间接影响到进程的运行。因而软件包之间的依赖关系也应该被考虑。

文献[34]采用了“分级分类”的标记方法对软件包的完整性进行标记,经过标记的软件包之间形成具有单向依赖关系的层次式结构。对应用软件包进行完整性标记后即可结合基于 Biba 模型[37]的强制访问控制策略与可信计算技术实现应用层次之间、类别之间的安全隔离,排除或减少环境中非预期的干扰。然而文献[34]虽然考虑到了进程运行对于内核的依赖,但是过于笼统地描述了保护方法。由于在操作系统中内核是由所有进程共享的,恶意进程对内核可以实施修改、挂钩或拦截,这样即使保证了上层软件包的安全性,不对内核进行可信度评估也无法保证进程执行环境的安全。

上述研究考虑到了进程执行的软件包依赖,但是仅对其直接依赖的软件包进行了可信度量,未对间接依赖的软件包进行可信度量,同时忽略了进程执行对系统内核的依赖关系,因此无法全面保障进程运行环境的可信。

2)进程运行时的可信度量方法

进程运行时可信主要是指进程内存空间中的数据结构的可信,主要包括代码段、栈和堆等。现有技术从不同的角度实

现对进程运行时的可信度量,但都存在一定的问题和不足。

StackGuard[38]在调用执行任意函数后,在栈中的返回地址前设置一个单字长的“canary”值以检测溢出攻击,当发现“canary”值被修改,则认为栈遭到了溢出攻击。但这种方法易被攻击者精心设计的溢出攻击绕过。

Stack shield[39]使用影子堆栈来监控函数的返回地址,以检测是否存在堆栈溢出攻击,通过修改系统的可执行程序加载器,在程序加载时在二进制可执行文件中重新写入监控代码,以监控程序的动态事件并进行记录。

Program shepherding[40]通过监控进程的控制流转移,以判定进程运行时是否可信。文献[41,42]通过基于静态分析提取程序的控制流图,在运行时监控程序的控制流转移是否符合控制流图,以确定进程运行时是否可信。

文献[43]通过截获客户操作系统中的系统调用来识别软件加载,并基于系统调用关联性分析和虚拟机文件系统元数据重构技术来验证客户操作系统中软件的完整性,设计并实现了一种在 VMM 层基于系统调用分析技术来验证软件完整性的方法 VMGuard。

文献[44]引入可信计算概念提出一种基于可信计算的动态完整性度量模型,在软件加载后对运行中的进程行为进行监控,动态度量其完整性。该模型能防止运行过程中恶意攻击破坏系统的完整性,从而提高系统安全性。

上述研究仅对进程内存空间的代码段等静态部分进行可信度量,无法满足定制安全交换中对进程运行时的栈、堆等动态部分进行可信度量的要求,难以保证专用交换进程的可靠运行。

综上所述,现有的网络连接技术无法从进程可信的角度来保护定制安全交换,且进程可信度量技术只对内存空间的静态部分进行可信度量,无法满足定制安全交换中对进程运行时动态可信度量的要求。因此下一步需要深入分析专用交换进程的可信度量方法,针对专用交换进程的执行环境可信度、运行时可信度展开研究。结合进程的执行对软件包和内核的依赖关系,研究专用交换进程执行环境可信度量算法,针对进程内存空间中的关键段研究专用交换进程运行时动态度量算法。

4 研究热点及发展前景

经过前期的不懈努力,定制数据安全交换技术取得了一定的成果。但从解决基于互联网电子政务信息安全交换的实际应用状况来看,该技术还未达到所期待的效果。下一步面向互联网电子政务的定制数据安全交换技术的研究热点和发展前景主要包括以下三个方面:

a)流交换。随着云计算、传感器网络、P2P 网络等大规模复杂网络的快速发展,对定制安全交换技术提出了新的挑战。交换的数据不再仅仅是静态的、固定大小的已知数据,而是一种连续的、无限的、快速的、随时间变化的、不可预测的流(如电视会议、实时监控、在线视频、股票交易等数据)。因此如何实现安全的流交换将会成为保障数据安全交换的关键,需要大家共同研究与探索。随着大数据时代的到来,流交换的安全性研究必将成为下一步的研究热点和难点。

b)交换进程行为评估模型优化。进程行为评估模型的建立是进程行为评估技术研究的核心,是目前进程行为评估的研究热点。如何对进程行为建模,使其能够准确地描述进程行为是研究的难点。现有的进程行为评估技术存在准确率低、误报率高的问题,只从建模方法对进程行为评估技术进行研究存在难度大、性能提升空间小的问题,并且对于如何选择一个合理的进程行为评估模型缺乏衡量标准。因此下一步需要结合政务系统之间数据交换的行为特征进一步研究专用交换进程行为模型优化和模型选取等问题。

c)科学合理地制定数据安全交换技术规范和标准。目前,我国基于互联网电子政务信息安全交换方面还没有采取统一的措施与方法,没有形成规范的、标准的基于互联网电子政务信息安全交换方法和手段,因此迫切需要有关部门加强协调,制定切实可行的统一的基于互联网电子政务信息安全交换技术规范和标准。通过制定科学合理的信息安全交换规范和准则,保证政务办公的内部数据处理区域和公开数据处理区域之间数据安全共享与交换,进一步提高政务对外提供服务的效率和能力。

5 结束语

定制数据安全交换主要用于解决面向互联网电子政务的异构环境下不同安全域间的数据安全共享与交换问题,保障信息共享、防止信息泄露和非授权访问。定制数据安全交换通过基于属性的加密技术,保证交换数据的保密性及细粒度访问控制;通过监管交换行为,保证专用交换进程的可信;通过受控的交换网络连接,在信息系统之间形成安全的交换链,保证所要交换的数据从交换链的源端到目的端的安全转移,并且限制非法交换链的建立。因此,研究定制数据安全交换的关键技术对实现互联网电子政务系统的信息共享、资源整合、满足信息共享的安全需求、消除“信息孤岛”等问题具有重要的作用和意义。

参考文献:

[1] 全国信息安全标准化技术委员会. GB/Z 24294,基于互联网电子政务信息安全实施指南[S]. 2009.

[2] Wikipedia. Cloud storage[EB/OL]. [2012-05-10]. http://en.wikipedia.org/wiki/Cloud_storage.

[3] BENALOH J, CHASE M, HORVITZ E, *et al*. Patient controlled encryption: ensuring privacy of electronic medical records[C]//Proc of ACM Workshop Cloud Computing Security. New York: ACM Press, 2009:103-114.

[4] DONG Chang-yu, RUSSELLO G, DULAY N. Shared and searchable encrypted data for untrusted servers[C]//Proc of the 22nd Conference on Data and Applications Security. Berlin: Springer, 2008:127-143.

[5] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology. Berlin: Springer, 2005:457-473.

[6] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006:89-98.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007:321-334.

[8] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007:456-465.

[9] GOYAL V, JAIN A, PANDEY O, *et al*. Bounded ciphertext policy attribute based encryption[C]//Proc of the 35th International Colloquium on Automata, Languages and Programming. Berlin: Springer, 2008:579-591.

[10] YU Shu-cheng, WANG Cong, REN Kui, *et al*. Attribute based data sharing with attribute revocation[C]//Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New

York:ACM Press, 2010.
[11] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//Proc of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008:417-426.
[12] IBRAIMI L, PETKOVIC M, NIKOVA S, *et al*. Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes[R]. Enschede:University of Twente, 2009.
[13] YU Shu-cheng, WANG Cong, REN Kui, *et al*. Achieving secure, scalable, and fine-grained data access control in cloud computing [C]//Proc of the 29th Conference on Information Communications. Piscataway: IEEE Press, 2010:534-542.
[14] NARAYAN S, GAGNE M, SAFAVI-NAINI R. Privacy preserving EHR system using attribute-based infrastructure[C]//Proc of ACM Cloud Computing Security Workshop. New York: ACM Press, 2010: 47-52.
[15] LIANG Xiao-hui, LU Rong-xing, LIN Xiao-dong, *et al*. Patient self-controllable access policy on phi in ehealthcare systems[C]//Proc of Advances in Health Informatics Conference. 2010.
[16] IBRAIMI L, ASIM M, PETKOVIC M. Secure management of personal health records by applying attribute-based encryption[R]. Enschede: University of Twente, 2009.
[17] LI Ming, YU Shu-cheng, REN Kui, *et al*. Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings[C]//Proc of the 6th International ICST Conference on Security and Privacy in Communication Networks. Berlin:Springer, 2010:89-106.
[18] CHASE M. Multi-authority attribute based encryption[C]//Proc of the 4th Conference on Theory of Cryptography. Berlin: Springer, 2007:515-534.
[19] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//Proc of the 16th ACM Conference on Computer and Communications Security. New York:ACM Press, 2009:121-130.
[20] LEWKO A, WATERS B. Decentralizing attribute-based encryption [C]//Advances in Cryptology-Eurocrypt. Berlin: Springer-Verlag, 2011:568-588.
[21] LI Ming, YU Shu-cheng, ZHENG Yao, *et al*. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. IEEE Trans on Parallel and Distributed Systems, 2013,24(1):131-143.
[22] FORREST S, HOFMEYR S A, SOMAYAJIA, *et al*. A sense of self for UNIX processes[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1996: 120-128.
[23] HOFMEYR S A, FORREST S, SOMAYAJI A. Intrusion detection using sequence of system calls[J]. Journal of Computer Security, 1998, 6(3): 151-180.
[24] WAGNER D, DEAN D. Intrusion detection via static analysis [C]// Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2001: 156-168.
[25] DEBAR H, BECKER M, SIBONI D. A neural network component for an intrusion detection system [C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1992: 256-266.
[26] ESKIN E, LEE W, STOLFO S. Modeling system call for intrusion detection with dynamic window sizes [C]//Proc of the 2nd DARPA Information Survivability Conference and Exposition. Washington DC: IEEE Computer Society, 2001: 165-175.
[27] WESPI A, DACIER M, DEBAR H. Intrusion detection using variable-length audit trail pattern [C]//Proc of the 3rd International Workshop on Recent Advances in Intrusion Detection. London: Springer-Verlag, 2000: 110-129.
[28] WARRENDER C, FORREST S, PEARLMUTTER B. Detecting intrusions using system calls: alternative data models [C]//Proc of IEEE Computer Society Symposium on Research in Security and Privacy. Washington DC: IEEE Computer Society, 1999: 133-45.
[29] LEE W, STOI FO S, MOK K. A data mining framework for building intrusion detection models [C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1999: 120-132.
[30] 吴瀛, 江建慧. 基于进程轨迹最小熵长度的系统调用异常检测[J]. 计算机应用, 2012,32(12):3439-3444,3452.
[31] 苗德成, 奚建清,苏锦钿. AADL 进程子集行为语义研究[J]. 计算机工程与科学, 2012,34(7):93-98.
[32] 张帆, 徐明迪,游林. 基于系统调用和进程代数 CCS 的行为建模方法[J]. 武汉大学学报:理学版, 2011,57(5):375-382.
[33] VASSILIOU P C G, VASILEIOU A. Asymptotic behaviour of the survival probabilities in an inhomogeneous semi-Markov model for the migration process in credit risk[J]. Linear Algebra and Its Applications, 2013,438(7):2880-2903.
[34] 陈亚莎, 胡俊, 沈昌祥. 可信应用环境的安全性验证方法[J]. 计算机工程, 2009, 37(23):152-154.
[35] 任江春, 王志英, 戴葵. 一种新的进程可信保护方法[J]. 武汉大学学报:理学版, 2006, 52(5): 532-536.
[36] 陈菊, 谭良. 一个基于进程保护的可信终端模型[J]. 计算机科学, 2011, 38(4): 114-117.
[37] BIBA K J. Integrity considerations for secure computer systems, MTR 3153[R]. [S. l.]: The Mitre Corporation, 1977.
[38] COWAN C, PU C, MAIER D, *et al*. StackGuard: automatic adaptive detection and prevention of buffer-overflow attacks[C]//Proc of the 7th USENIX Security Symposium. 1998: 346-355.
[39] Stack shield[EB/OL]. (2000-01-08). http://www. angelfire. com/sk/stackshield/.
[40] KIRIANSKY V, BRUENING D, AMARASINGHE S. Secure execution via program shepherding[C]//Proc of the 11th USENIX Security Symposium. 2002: 191-206.
[41] ABADI M, BUDIU M, ERLINGSSON Ú, *et al*. Control-flow integrity principles, implementations, and applications[J]. ACM Trans on Information and System Security, 2009, 13(1):1-40.
[42] CASTRO M, COSTA M, HARRIS T. Securing software by enforcing data-flow integrity[C]//Proc of the 7th Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2006: 147-160.
[43] 李博, 李建欣, 胡春明,等. 基于 VMM 层系统调用分析的软件完整性验证[J]. 计算机研究与发展, 2011,48(8): 1438-1446.
[44] 杨蓓, 吴振强, 符湘萍. 基于可信计算的动态完整性度量模型[J]. 计算机工程, 2012,38(2):78-81.

(上接第 964 页)

[31] HAIDAR A, LTAIEF H, LUSZCZEK P A, *et al*. Comprehensive study of task coalescing for selecting parallelism granularity in a two-stage bidiagonal reduction [C]//Proc of the 26th IEEE International Parallel and Distributed Processing Symposium. Washington DC: IEEE Computer Society, 2012: 25-35.
[32] SAIFULLAH A, LI Jing, AGRAWAL K, *et al*. Multi-core real-time scheduling for generalized parallel task models [J]. Real-Time Systems, 2013,49(4):404-435.
[33] HU J, MARCULESCU R. Communication and task scheduling of application-specific networks-on-chip [J]. IEE Proceedings of Computers and Digital Techniques, 2005, 152(5): 643-651.
[34] WANG Yi, LIU Duo, WANG Meng, *et al*. Optimal task scheduling by removing inter-core communication overhead for streaming applications on MPSoC [J]. IEEE Trans on Computers, 2013, 62(2): 336-350.
[35] VARATKAR G, MARCULESCU R. Communication-aware task scheduling and voltage selection for total systems energy minimization [C]//Proc of International Conference on Computer-Aided Design. Washington DC: IEEE Computer Society,2003:510-517.
[36] GRUIAN F, KUCHCINSKI K. Low-energy directed architecture selection and task scheduling for system-level design [C]//Proc of the 25th EUROMICRO Conference. 1999: 296-302.
[37] WANG Ying-feng, LIU Zhi-jing. Joint communication and processor frequency selection for low-energy systems under timing constraints [J]. China Communications, 2010, 7(4): 132-136.