软件系统的可信降密述评

朱 浩[1,2] 陈建平[1]
(南通大学计算机科学与技术学院 江苏 南通 226019)[1]
(南京航空航天大学计算机科学与技术学院 南京 210016)[2]

摘 要 无干扰模型是信息流控制中的基础性安全模型,能确保敏感信息的零泄露,但其安全条件的限制性过强。软件系统由于功能的需要不可避免地需要违反无干扰模型,释放合适的信息。为了防止攻击者利用信息释放的通道获取超额的信息,需要对释放的通道进行控制,建立信息可信降密的策略和实施机制。基于不同维度对现有的降密策略进行归类,大致归并为降密的内容、主体、地点和时间维度;并对现有降密策略的实施机制进行分类,大致可分为静态实施、动态实施和安全多次执行;对这些机制的特点和不足之处进行比较,并探讨了后续研究面临的挑战,展望了未来的研究方向。

关键词 可信降密,信息流控制,无干扰,机密性
中图法分类号 TP311 **文献标识码** A

Review of Trust Declassification for Software System

ZHU Hao[1,2] CHEN Jian-ping[1]
(School of Computer Science and Technology, Nantong University, Nantong, Jiangsu 226019, China)[1]
(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[2]

Abstract Non-interference model is the baseline security model of information flow control. It ensures zero leakage of secret information, but its restrictiveness of security condition is too strong. Software system inevitably violates non-interference model and releases proper information for its requirement of function. In order to prevent attacker obtain extra information from the channel of information release, the channel should be under control and trusted declassification policy and enforcement mechanisms should be established. Existing declassification policies are classified into WHAT, WHO, WHERE and WHEN dimensions, and existing enforcement mechanisms are classified into static enforcement, dynamic enforcement and secure multi-execution. The characteristics and deficiencies of these mechanisms were compared, the challenge of following study was discussed, and the direction of future study was out-looked.

Keywords Trusted declassification, Information flow control, Non-interference, Confidentiality

1 引言

信息可信降密研究的是如何确保敏感信息的可信释放[1-2],关注的是软件可信属性中的保密性[3-4]。传统的加密和访问控制技术不能完全确保端到端的保密性。加密技术通过系统外部研究安全问题,能在一定程度上确保数据通过传输信道安全地从发送方到达指定接收方,但是不能保证数据在接收方被解密后在计算过程中其保密性不遭破坏。比如,解密后的数据由于软件缺陷原因被无意地泄漏。全同态加密方案能在计算过程中对用户数据提供保护,但是它非常消耗计算资源[5-6]。传统的访问控制技术通过系统的边界研究安全问题,能控制信息的访问,但是不能控制信息的传播。如果一个应用程序被允许读一些敏感数据,那么很难控制它如何分发这些已经读到的数据[7]。信息流控制从系统内部研究信息的传播问题,是一种以数据为中心的安全机制[8]。它通过信息流控制策略和实施机制来控制信息的传播,力图实现端到端的安全。信息可信降密属于信息流控制的研究范畴。

可信降密模型是一种放松的无干扰安全模型。无干扰模型是信息流控制中一个非常重要的基础性安全模型[9],它的主要思想是低安全级别的输出不依赖于高安全级别的输入,使得攻击者无法从低安全级别的输出中推导出高安全级别的输入。无干扰模型的原理如图 1 所示,其中,h_1 和 h_2 是高安全等级的输入,l 是低安全等级的输入,h_1' 和 h_2' 是高安全等级的输出,l' 是低安全等级的输出。

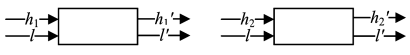

图 1 无干扰模型

从保密性角度而言,无干扰模型能保证敏感信息的零泄漏,但在现实场景中,它的限制性太强,很多系统不可避免地会违反无干扰,有意释放一些敏感信息,否则没有实用意义。比如,登录口令检查程序拒绝错误口令登录,但拒绝行为本身却释放了一定量的信息,排除了一个错误的口令,缩小了口令

本文受江苏省博士后科研资助计划(1401022C),南通大学博士科研启动基金(14B22)资助。
朱 浩(1977-),男,博士,副教授,CCF 会员,主要研究方向为软件安全,E-mail:searain@nuaa.edu.cn(通信作者);陈建平(1960-),男,教授,主要研究方向为数值计算与隐私保护。

有学生的这些度量值的平均值、极差、平均差、极差系数和平均差系数。

2.4 学习效果的评估

基于学习情感演化模型，单个样本知识点的学习效果评估方法为：1)学习情感为积极情感和中性情感所占比例尽可能大，学习情感值的平均值尽可能大；2)学习情感值的极差、平均差、极差系数和平均差系数尽可能小。

对于两个知识点，学习效果的评估方法为：1)学习情感极性从负面转变为正面所占的比例尽可能大，学习情感极性从正面转变为负面所占的比例尽可能小；2)学习情感值的变化值为非负数所占的比例尽可能大，学习情感值变化值为负数所占的比例尽可能小；3)学习情感值变化值的平均值、极差、平均差、极差系数和平均差系数尽可能小。

对于每名学生或所有学生的知识点关系路径，即统计对象为 X_3，X_4，X_5，X_6，X_7，X_8，X_9，X_{10} 中的元素，学习效果的评估方法为：1)关于知识点关系路径上学习情感值的度量指标中，平均值尽可能大，极差、平均差、极差系数和平均差系数尽可能小；2)在关于知识点关系路径上学习情感值的变化值的度量指标中，平均值、极差、平均差、极差系数和平均差系数应尽可能小。

结束语 教师不仅承担以认知教育为目标的教学任务，而且承担情感教育的重任。本文旨在通过学习者对知识点、知识点关系路径的学习情感值及其变化值来评估学习效果。为此，首先构建了细粒度学习情感本体、细粒度学习情感课程本体，它们以知识点为学习情感的认知单元，刻画了知识点的相关特性，包括类型和认知目标等，形成了面向知识点的学习情感分类和教师情感反馈行为分类框架；然后提出了一种基于细粒度学习情感本体的学习效果评估方法，该方法通过学习情感演化模型来描述面向知识点及其关系路径的学习情感变化的特点和规律，进而评估学生的学习效果。本文所提基于细粒度学习情感本体的学习效果评估方法不但能够作为教师评价学习效果的手段，而且能够发现学生的薄弱知识点，加强学习的针对性和目的性，从而提高教学效果。

参 考 文 献

[1] 耿显亚. 影响高校数学学习的情感因素分析[J]. 教育教学论坛，2014，6(18)：102-103.

[2] BLOOM B S，ENGELHART M D，FURST E J，et al. Taxonomy of Educational Objectives：The Classification of Educational Goals. Handbook I：Cognitive Domain [M]. New York：Longman，1956.

[3] 刘万友. 网络教育和传统教育之比较[J]. 科技信息，2007，25(14)：164.

[4] 邓妍祯，莫建萍. 积极情感因素在网络自主学习中的作用及培养途径分析[J]. 中国电力教育，2014，30(32)：52-53.

[5] 邓铁辉. 教师教学正面情感的提高与差生学习负面情感的消除[J]. 湖南科技学院学报，2015，36(7)：146-147.

[6] 沈映珊，汤庸. 社交学习网络中基于学习认知的情感交互研究[J]. 现代教育技术，2015，25(9)：90-96.

[7] 陶小梅，牛秦洲. 基于情感学习本体的教学反馈策略生成算法的研究[J]. 计算机工程与科学，2015，37(2)：320-328.

[8] 盛群力，褚献华. 布卢姆认知目标分类修订的二维框架[J]. 课程教材教法，2004，24(9)：90-96.

[9] 唐晓波，朱娟，杨丰华. 基于情感本体和 KNN 算法的在线评论情感分类研究[J]. 信息系统，2016，39(6)：110-114.

[10] ANDERSON L W，KRATHWOHL D R，AIRASIAN P W，et al. A Taxonomy for Learning，Teaching and Assessing：A Revision of Bloom's Taxonomy of Educational Objectives [M]. New York：Longman，2001.

[11] EKMAN P. Chapter 3：Basic Emotions. DALGLEISH T and POWER MJ. Handbook of Cognition and Emotion[M]. Chichester：John Wiley & Sons，2000.

[12] ECONOMIDESA A. Emotional Feedback in CAT[J]. International Journal of Instructional Technology & Distance Learning，2006，3(2)：11-20.

[13] EKMAN P. An Argument for Basic Emotions[J]. Cognition and Emotion，1992，6(3/4)：169-200.

(上接第 45 页)

[11] STUCKEY P J，FEYDY T，SCHUTT A，et al. The MiniZinc Challenge 2008-2013 [J]. AI Magazine，2014，35(2)：55-60.

[12] SABIN D，FREUDER E C. Contradicting Conventional Wisdom in Constraint Satisfaction[C]// Proceedings of CP-1994. 1999：10-20.

[13] GRANDONI F，ITALIANO G F. Improved Algorithms for Max-restricted Path Consistency [C]// Principles & Pratice of Constraint Programming-cp. Kinsale：Cp，2003：858-862.

[14] VION J，DEBRUYNE R. Light Algorithms for Maintaining Max-RPC During Search [C]// Proceedings of SARA'09. 2010：167-174.

[15] HARALICK R M，ELLIOTT G L. Increasing Tree Search Efficiency for Constraint Satisfaction Problems [J]. Artificial Intelligence，1980，14(3)：263-313.

[16] DECHTER R，MEIRI I. Experimental Evaluation of Preprocessing Techniques in Constraint Satisfaction Problems[C]// International Joint Conference on Artificial Intelligence (IJCAI-1989). 1989：271-277.

[17] BALAFOUTIS T，PAPARRIZOU A，STERGIOU K，et al. New Algorithms for Max Restricted Path Consistency [J]. Constraints，2011，16(4)：372-406.

[18] Christophe Lecoutre[EB/OL]. http://www.cril.univ-artois.fr/~lecoutre/benchmarks.html.

[19] 崔佳旭. Mistral 求解器扩展与应用研究[D]. 长春：吉林大学，2016.

的搜索空间;再如,假设公司中每个员工的工资信息是敏感信息,某程序需要向外界公开该公司的平均工资水平,工资的平均值将释放员工工资的部分信息。因此,某些情况下敏感信息的释放是可以容忍的或者是程序功能需要的,但是攻击者会利用这种释放通道窃取超额的敏感信息。对于上例,如果不加限制,攻击者利用暴力破解,不断尝试口令登录,不断缩小口令搜索空间,直到尝试成功;攻击者可以通过代码注入攻击,利用平均工资的释放通道窃取每个员工的工资信息。因此,需要对敏感信息的释放通道进行控制,确保合适的主体在合适的时间和地点释放合适的敏感信息,这个控制过程被称为信息的可信降密[1]。对于登录口令检查程序,可以限定错误密码尝试登录的次数;对于平均工资的释放通道,可以建立信息降密的安全模型、策略和机制,防止非法信息的释放。

2　降密的维度

Sabelfeld 等人总结了信息可信降密的研究主要集中在内容、地点、主体以及时间等维度,通过这些维度试图解决"什么信息可以降密""在哪儿降密""谁能降密"以及"降密的时间"等一系列问题[1]。基于这些维度,本节简要回顾各个维度的研究现状。

(1)内容维度方面。文献[10-11]基于一种部分等价关系模型(Partial Equivalence Relation Model,PER)提出了选择性信息降密策略,规定了信息中允许被释放的部分,比如某应用程序需要打印银行卡号,则可以利用该策略选择银行卡号的部分数字进行打印,而另外的部分则保密。文献[12]提出的"定界释放"(delimited release)策略使用"逃逸舱"来释放敏感信息。"逃逸舱"是高安全级别信息降密的唯一通道,它的功能由语句 declassify(e)来实现,其中 e 是需要降密的表达式,该语句执行后,e 的值将完全公开。"定界释放"策略规定:程序中高安全级别信息的变化不能引起"逃逸舱"中需要降密的表达式值的变化,从而使得攻击者无法从可观察的输出中反向推导出高安全级别的信息。文献[13]提出通过设置"释放哨"(declassification guard)来明确地声明释放的内容,能有效地检测出"定界释放"策略不能识别的攻击。文献[14]基于信息格研究了计算系统中合法信息流的条件,该策略模型能将基于部分等价关系模型、集合论以及信息论等描述的信息流策略统一起来,提供了一个策略描述和实施的统一框架,该框架能用来实施内容维度的释放策略。文献[15]则基于应用程序的交互机制,提出了交互式降密策略,由用户来决定释放的内容。文献[16]提出了一个应用程序表达无干扰和内容维度降密性质的框架,其中降密的内容由输入的消息提供。

(2)地点维度方面。非传递无干扰模型[17-20]一般包含 3 个安全层次:保密层、公开层和降密层。降密层处于中间,保密层的信息如果需要流入公开层,则必须首先经过降密层处理。非传递无干扰可以扩展到任意多个安全层次。文献[21]基于非传递无干扰提出了一个更细粒度的基于地点维度的信息降密策略,并给出了一个静态实施的类型系统。Hicks 等人[22]提出将程序文件和全局策略文件分开存储,统一编译,在全局策略中定义了若干释放函数,各个实体在全局策略中声明其所信任的释放函数以及各个实体之间的委托关系,各个实体仅能通过它们所信任的释放函数来释放信息。Askarov 等人[23]提出了"渐进释放"(gradual release)策略,限定敏感信息仅能在特定的程序点释放,除此之外在任意程序点释放敏感信息都是非法的。

(3)主体维度方面。文献[24]引入了"流锁"(flow locks)的概念,程序中每个变量都有一个可以读取该变量的主体集合,其中的每个主体可以通过一个逻辑开关(即"流锁")来决定该主体是否具有读取这个变量的权限。策略中引入了 open 语句和 close 语句来对"流锁"实施打开和关闭操作。Myers 等人[25]提出了分散式标签模型(Decentralized Label Model,DLM),它能在各个主体相互不信任的环境中实施信息流控制策略。在该模型中,安全策略并不是由授权中心确定,而是由每个主体自己定义的本地安全策略确定,整个系统的行为必须遵循所有主体的本地策略。各个主体通过标签来表达安全需求,每个标签是由若干个单独的访问控制规则构成的集合。访问控制规则具有(owner:readers)形式,其中 owner 是数据的所有者,readers 是这个访问控制规则允许读该数据的主体的集合。每个主体可以通过向标签的访问控制规则中加入读者的方法来表达自己允许释放信息的要求,但是由于系统的运行必须符合所有的访问控制规则,因此只有当数据的所有访问控制规则都同意向某特定读者释放该数据时,释放才能真正有效。分散式标签模型 DLM 已经在安全类型语言 JRIF[26]的编译器中实现。文献[27]提出了鲁棒性降密策略:主动攻击者(能够观察和修改被攻击系统的行为)不能获得比被动攻击者(仅能观察被攻击系统的行为)更多的敏感信息。在后续的研究中,Myers 等人[28]结合了完整性约束,对鲁棒性策略重新进行了表述:主动攻击者不能通过修改程序的低完整性代码来影响降密语句是否会被执行以及降密的内容。但是在一些应用场景中,比如信息购买场景,用户的选择将影响降密的内容,因此有必要为一些低完整性代码赋予有限的能力来影响降密。鉴于此,文中又提出了受限的鲁棒性策略,引入 endorsement 原语来提升低完整性代码的完整性级别,以屏蔽相应策略的检查,从而赋予低完整代码一定的能力来影响降密的内容。但是,上述研究只考虑了程序运行终止的情况。为此,Askarov 等人[29-30]将鲁棒性策略扩展到程序运行非终止的情况,并对攻击者的控制能力和攻击影响进行了形式化描述,提出了一个更精确的鲁棒性的条件。

(4)时间维度方面。Volpano 和 Smith[31-32]基于时间复杂度提出了"如果攻击者不能在多项式时间内获得敏感信息,那么系统就满足无干扰性质"的观点。但是,这种无干扰仅仅是在多项式时间内是成立的,在多项式时间之外,攻击者能获取敏感信息。Chong 和 Myers[33]将每个变量都标记有相应的降密策略,其中制定了降密发生的条件,比如在用户购买信息中,只有当确认收到用户的付款后,才能把相应的信息释放给用户。文献[34]提出了一个在竞标系统中支持降密的安全策略框架,每一个降密步骤由相应的降密操作来标识,当设定的条件满足时,降密步骤中规定的降密操作才能执行。

3　降密的实施机制

3.1　静态实施

类型系统是一种静态实施机制[35]。它在程序执行之前对程序中的信息流进行分析,通过建立策略的类型规则系统对程序进行类型推导,推导结果为良类型(well-typed)的程序满足相应的降密策略。静态实施方法关注程序的所有执行路

径,但由于缺乏对程序所有执行路径的实时验证能力,往往只能做最保守的近似估计,从而导致对策略约束条件的限制性过强,通常将满足安全策略的程序误判为不安全的。静态实施方法发生在程序运行之前,不会增加系统的运行负载。在第 2 节回顾的不同维度的降密策略中,“定界释放”[12]“渐进释放”[23]和“鲁棒性降密”[27]等策略都采用了类型系统的实施机制。

除了类型系统,模型检测的方法也被用来静态实施降密策略。孙聪等人[36-37]提出了一种基于下推系统可达性分析的高效验证方法,并对“定界释放”策略[12]进行了分析和验证,实验表明该方法具有比类型系统更高的精确性。文献[38]提出了一种基于符号执行的方法来验证 Android APP 中的交互式降密策略,实验表明该方法能有效检测移动 Android APP 中的非法信息泄漏。

3.2 动态实施

动态监控方法是在程序的执行过程中由监控器对程序中的信息流进行合法性检查,当运行非法信息流的程序命令时,监控器能采取相关措施来确保信息的安全,比如终止程序的执行,或者将不安全的程序命令转化为安全的程序命令等[39]。动态监控方法关注的是程序当前的执行路径,能提供更加宽容的实施机制,但是它发生在程序的执行过程中,会增加系统的运行负载。随着计算机硬件性能的不断提高,动态监控方法的运行负载所带来的影响正不断减小,其在信息流控制领域有广泛的应用[40-41]。文献[42]提出了一种实施降密策略的动态监控机制,并对其进行了可靠性分析。文献[43]则提出了一种结合静态和动态方法的混合实施机制,用于实施内容和地点维度的降密策略。

内嵌式引用监控(In-lined reference monitor)方法[44]通过一个可信的重写进程将实施安全策略的代码嵌入到目标应用程序中,生成了一个新的应用程序,该程序的执行不需要外部监控器,能实现自我监控,并且遵循嵌入的安全策略。该方法能实施丰富的安全策略,适应异构的分布式监控环境,但也有增加系统资源消耗的缺陷。文献[45]基于内联引用监控方法,实施了基于内容和地点维度的二维降密策略,并证明了该方法的可靠性。

3.3 安全多次执行

除了静态和动态实施以外,还有一种新的实施机制:安全多次执行(secure multi-execution)[46-47]。它的基本思想是:在不同的安全等级下多次执行程序,低安全等级的执行只能处理低安全等级的事件,高安全等级的执行可以处理所有安全等级的事件,不同安全等级的输出通道只能在各自安全等级的执行状态下输出信息。安全多次执行能用来实施内容和时间维度的降密策略[47]。

4 挑战与展望

4.1 面临的挑战

目前该领域的研究面临着如下挑战。

(1)信息降密的研究集中在不同的维度上,单一维度的降密策略只关注信息降密某一方面的安全条件,而忽视了其他维度的安全限制,因此攻击者会利用其他维度的漏洞进行“信息清洗攻击”(information laundering attack),从而非法获取敏感信息。因此,信息可信降密需要综合考虑多个维度来提高抵抗“信息清洗攻击”的能力。

目前,维度集成方面的研究大多能集成两个维度。文献[48]扩展了内容维度的“定界释放”策略,提出了集成内容和地点两个维度的“本地化定界释放”策略,其在一定程度上保证了在恰当的程序点释放合适内容的信息。文献[49]同样扩展了内容维度的“定界释放”策略,提出了集成内容和主体维度的“分散式定界降密”策略,该策略从一定程度上确保了由恰当的主体释放合适内容的信息。信息降密的各个维度是彼此正交的,提出无缝集成更多维度的信息降密模型是该研究领域的一个重要挑战之一。

(2)信息降密的研究集中在单线程顺序式程序设计语言环境中,而多线程是现代程序设计语言的一个重要特征,因此将单线程环境中的不同维度的信息降密模型扩展到多线程并发环境中是一项非常有意义的工作。文献[50]将内容维度的降密策略扩展到多线程环境;文献[51]将基于内容和地点维度的降密策略扩展到多线程环境。在后续的研究中,多线程中的降密策略一方面需要集成更多的维度;另一方面需要防止线程调度所产生的时间隐通道,避免信息被非法释放。

(3)信息降密的研究集中在程序内部变量级别,降密的实施机制普遍采用基于程序设计语言的机制[1-2]。这些研究工作把降密问题置于软件开发的后期进行考虑,主要集中在程序的编译阶段和程序运行时的监控阶段,在这些阶段考虑降密问题存在一定的滞后性,带来的问题是程序员的编程负担加重、程序设计语言的编译器和动态运行环境都需要扩展以及缺乏从宏观视野考虑软件架构层面的降密问题。

(4)目前,降密策略静态实施机制研究主要集中在类型系统和模型检测,类型系统具有限制性过强的缺点,而模型检测存在空间状态爆炸问题。定理证明方法可以避免这些问题,因此,用定理证明方法实施降密策略是一项非常有意义和具有挑战性的工作。

4.2 展望

软件架构层面的信息可信降密问题值得探索。软件架构非常类似于建筑物的架构,它是一个软件从整体到部分的最高层次的划分和组织。一旦在软件架构层做出决定,在软件后期的开发和维护过程中,这种架构上的决定一般很难更改甚至无法更改。因此,软件架构的设计是软件设计中最重要的环节之一,必须慎重考虑。

基于组件的软件工程将软件视为由若干组件构成,那么软件的架构就表现为各个组件之间的结构和关系,不同的结构和关系会对软件整体的性能造成不同的影响。另外,随着软件复杂度的提高,不同的组件可能来自不同的第三方,当这些来源不同的组件粘合在一起构成一个软件系统时,如何确保敏感信息不被非法窃取是一个非常重要的问题。比如,日益流行的新型的 Web 应用程序 Mashup 整合了若干个第三方 Mashup 组件服务而构建了一个新的服务,那么如何防止各个 Mashup 组件之间敏感信息的泄漏则是一个亟待解决的问题。由此可见,安全问题需要立体纵深防御,需要从不同层面考虑安全问题。信息可信降密问题也需要从软件的架构层面进行考虑。

文献[52]基于软件架构层,从非传递无干扰的角度考虑了信息降密的地点维度,但尚未考虑可信降密的其他维度。目前这方面的理论基础非常薄弱,需要从不同维度研究软件

架构中各个组件之间敏感信息的释放,从软件架构层建立信息可信降密的策略和机制,确保合适的主体在合适的时间和地点释放合适的内容。

下一步计划将信息可信降密问题置于软件开发的前期进行考虑,在软件的架构阶段就开始考虑可信降密的需求,建立满足可信降密需求的软件架构模型,然后通过模型驱动的思想进行模型的不断求精转换,并在模型转换过程中保持可信降密的安全性质,最终生成满足降密性质的框架代码。

结束语　信息流控制是研究软件系统保密性的重要方法之一,信息可信降密是信息流控制的研究范畴。信息可信降密模型放松了无干扰模型的限制条件,允许程序由于功能需要而进行信息的可控释放。为此,需要研究可信降密的策略和实施机制。本文对不同维度的降密策略和不同类型的实施机制进行归类比较,总结了目前存在的问题,展望了后续的研究方向:将信息可信降密问题置于软件架构层,并基于模型驱动的方法进行探讨。

参 考 文 献

[1] SABELFELD A,SANDS D. Declassification:dimensions and principles[J]. Journal of Computer Security,2009,7(5):517-548.

[2] 姜励. 基于程序设计语言的安全降密模型研究[D]. 杭州:浙江大学,2008.

[3] 沈昌祥,张大伟,刘吉强,等. 可信 3.0 战略:可信计算的革命性演变[J]. 中国工程科学,2016,18(6):53-57.

[4] 沈国华,黄志球,谢冰,等. 软件可信评估研究综述:标准、模型与工具[J]. 软件学报,2016,27(4):955-968.

[5] ZHANG L,ZHENGY,KANTOA R. A Review of Homomorphic Encryption and its Applications[C]//Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. Xi'an,ICST,2016:97-106.

[6] VAN DIJK M,JUELS A. On the impossibility of cryptography alone for privacy-preserving cloud computing[C]// 5th USENIX Conference on Hot topics in security (HotSec'10). Washington, USENIX Association,2010:1-8.

[7] SABELFELD A,MYERS A C. Language-based information flow security[J]. Selected Areas in Communications,2006,21(1):5-19.

[8] ALAM MI,HALDER,R. Data-Centric Refinement of Information Flow Analysis of Database Applications[C]// Proceedings of the Third International Symposium on Security in Computing and Communications. Kochi,Springer International Publishing,2015:506-518.

[9] GOGUEN J A,MESEGUER J. Security policies and security models[C]// Proceedings of IEEE Symposium on Security and Privacy. Oakland:IEEE,1982:11-20.

[10] COHEN E. Information transmission in computational systems [J]. ACM SIGOPS Operating Systems Review,1977,11(5):133-139.

[11] SABELFELD A,SANDS D. A per model of secure information flow in sequential programs[J]. Higher-order and Symbolic Computation,2001,14(1):59-91.

[12] SABELFELD A,MYERS A. A Model for Delimited Information Release[M]// Software Security-Theories and Systems. Springer Berlin Heidelberg,2004:174-191.

[13] LUX A,MANTEL H. Declassification with explicit reference points[C]// 14th European Conference on Research in Computer Security. Saint-Malo:Springer-Verlag,2009:21-23.

[14] ADETOYE A,BADII A. A Policy Model for Secure Information Flow[M]// Foundations and Applications of Security Analysis. Springer-Verlay,2009:1-17.

[15] MICINSKI K,FETTER-DEGGES J,JEON J,et al. Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution[C]// Proceedings of the 20th European Symposium on Research in Computer Security. Vienna:Springer International Publishing,2015:520-538.

[16] GREINER S,GRAHL D. Non-interference with What-Declassification in Component-Based Systems[C]// Proceedings of the 2016 IEEE 29th Computer Security Foundations Symposium (CSF). Lisbon:IEEE,2016:253-267.

[17] HAIGH J T,KEMMERER RA,MCHUGH J,et al. An experience using two covert channel analysis techniques on a real system design [C]// 1986 IEEE Symposium on Security and Privacy. IEEE,1987:14.

[18] RUSHBY J. Noninterference,transitivity,and channel-control security policies:CSL-92-02[R]. Menlo Park:SRI International Computer Science Laboratory,1992.

[19] BALDAN P,BEGGIATO A. Multilevel Transitive and Intransitive Non-interference,Causally[C]// Proceedings of the 18th IFIP WG 6.1 International Conference. Greece:Springer International Publishing,2016:1-17.

[20] EGGERT S,VAN DER MEYDEN R. Dynamic intransitive Noninterference revisited[M]// Formal Aspects of Computing,2017,29(4):1-34.

[21] MANTEL H,SANDS D. Controlled declassification based on intransitive noninterference [M]// Programming Languages and Systems. Springer Berlin Heidelberg,2004:129-145.

[22] HICKS B,KING D,MCDANIEL P,et al. Information release:high-level policy for a security-typed language [C]// Proceedings of the 2006 Workshop on Programming Languages and Analysis for Security. Ottawa: ACM Computer Society Press,2006:65-74.

[23] ASKAROV A,SABELFELD A. Gradual Release:Unifying Declassification,Encryption and Key Release Policies[C]// Proceedings of IEEE Symposium on Security and Privacy. Berkeley,CA:IEEE Computer Society Press,2007:207-221.

[24] BROBERG N,SANDS D. Flow locks:Towards a core calculus for dynamic flow policies[M]// Programming Languages and Systems. Springer Berlin Heidelber,2006:180-196.

[25] MYERS A C,LISKOV B. Protecting privacy using the decentralized label model [J]. ACM Transactions on Software Engineering and Methodology (TOSEM),2000,9(4):410-442.

[26] KOZYRI E,ARDEN O,AC MYERS. JRIF:Reactive Information Flow Control for Java[EB/OL]. (2016-02-12)[2017-8-21]. https://ecommons. cornell. edu/handle/1813/41194.

[27] ZDANCEWIC S,MYERS A C. Robust declassification[C]// Proceedings of IEEE Computer Security Foundations Workshop. Cape Breton:IEEEComputer Society Press,2001:15-23.

[28] MYERS A C,SABELFELD A,ZDANCEWIC S. Enforcing robust declassification and qualified robustness[J]. Journal of Computer Security,2006,14(2):157-196.

[29] ASKAROV A,MYERS A. A semantic framework for declassifi-

cation and endorsement[C]// European Conference on Programming Languages and Systems. Springer-Verlag,2010:64-84.
[30] ASKAROV A,MYERS A. Attacker control and impact for confidentiality and integrity[J]. Logical Methods in Computer Science,2011,7(3):563-572.
[31] VOLPANO D,SMITH G. Verifying secrets and relative secrecy [C]// Proceedings of 27th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. Boston, MA: ACM Computer Society Press,2000:268-276.
[32] VOLPANO D. Secure introduction of one-way functions[C]// Proceedings of 13th IEEE Computer Security Foundations Workshop. Cambridge: IEEE Computer Society Press, 2000: 246-254.
[33] CHONG S,MYERS A C. Security policies for downgrading [C]// 11th ACM Conference on Computer and Communications Security. Washington DC:ACM Computer Society Press,2004:198-209.
[34] YAO J,TANG Y. Security Downgrading Policies for Competitive Bidding System[M]// Software Engineering and Knowledge Engineering:Theory and Practice. Springer Berlin Heidelberg, 2012:587-95.
[35] 吴泽智,陈性元,杨智,等. 信息流控制研究进展[J]. 软件学报, 2017,28(1):135-159.
[36] 孙聪,唐礼勇,陈钟. 基于下推系统可达性分析的程序机密消去机制[J]. 软件学报,2012,23(8):2149-2162.
[37] 孙聪,唐礼勇,陈钟. 基于下推系统可达性分析的输出信道信息流检测[J]. 计算机科学,2011,38(7):103-107.
[38] MICINSKI K,FETTER-DEGGES J,JEON J,et al. Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution[C]// Proceedings of 20th European Symposium on Research in Computer Security. Vienna:springer International Publishing,2015:520-538.
[39] SABELFELD A,RUSSO A. From dynamic to static and back: Riding the roller coaster of information-flow control research [M]// Perspectives of Systems Informatics. Springer Berlin Heidelberg,2010,5947:352-365.
[40] SHROFF P,SMITH S,THOBER M. Dynamic Dependency Monitoring to Secure Information Flow[C]// Proceedings of the 20th IEEE Symposiumon Computer Security Foundations. Venice:IEEEComputer Society Press,2007:203-217.
[41] RUSSO A,SABELFELD A. Securing timeout instructions in web applications[C]// Proceedings of the 22nd IEEE Symposium on ComputerSecurity Foundations. Port Jefferson: IEEE Computer Society Press,2009:92-106.
[42] 金丽,朱浩. 基于自动机监控的二维降密策略[J]. 计算机科学, 2015,42(7):194-199.
[43] ASKAROV A,SABELFELD A. Tight enforcement of information-release policies for dynamic languages[C]// Proceedings of the 25nd IEEE Symposium on ComputerSecurity Foundations. Port Jefferson:IEEE Computer Society Press,2012:43-59.
[44] SRIDHAR M,HAMLEN K W. Flexible in-lined reference monitor certification:challenges and future directions[C]// Proceedings of the 5th ACM Workshop on Programming Languages Meets Program Verification. Austin,Texas:ACM,2011:55-60.
[45] 朱浩,陈建平,金丽. 二维降密策略的内联引用监控方法[J]. 计算机科学,2016,43(11A):352-354.
[46] BOLO I,GARG D. Asymmetric Secure Multi-execution with Declassification[C]// Proceedings of the 5th International Conference on Principles of Security and Trust. Netherlands:Springer-Verlag New York,2016:24-45.
[47] VANHOEF M,GROEF W D,DEVRIESE D,et al. Stateful Declassification Policies for Event-Driven Programs[C]// Proceedings of the 2014 IEEE 27th Computer Security Foundations Symposium. Vienna:IEEE Computer Society,2014:293-307.
[48] ASKAROV A,SABELFELD A. Localized delimited release: Combining the what andwhere dimensions of information release [C]// Proceedings of the 2007 Workshop on Programming Languages and Analysis for Security. San Diego:ACM,2007:53-60.
[49] MAGAZINIUS J,ASKAROV A,SABELFELD A. Decentralized delimited release[C]// Proceedings of the 9th Asian Conference on Programming Languages and Systems. Kenting,Taiwan:Springer-Verlag,2011:220-237.
[50] 姜励,陈健,平玲娣,等. 多线程程序的信息抹除和降密安全策略 [J]. 浙江大学学报(工学版),2010,44(5):854-862.
[51] 金丽,朱浩. 多线程环境中的二维降密策略[J]. 计算机科学, 2015,42(12):243-246,282.
[52] VAN DER MEYDEN R. Architectural refinement and notions of intransitive noninterference [J]. Formal Aspects of Computing,2012,24(4):769-792.

(上接第 15 页)

[47] GREFF K,SRIVASTAVA R K,KOUTNÍK J,et al. LSTM:A Search Space Odyssey[J]. IEEE Transactions on Neural Networks & Learning Systems,2015,28(10):2222-2232.
[48] 杨红红,曲仕茹. 基于稀疏约束深度学习的交通目标跟踪[J]. 中国公路学报,2016,29(6):253-261.
[49] 司朋举,胡伟. 深度学习在仿生眼监控系统中的应用[J]. 测控技术,2016,35(12):139-143.
[50] 王慧燕,杨宇涛,张政,等. 深度学习辅助的多行人跟踪算法[J]. 中国图象图形学报,2017,22(3):349-357.
[51] 文孟飞,胡超,刘伟荣. 一种基于深度学习的异构多模态目标识别方法[J]. 中南大学学报(自然科学版),2016,47(5):1580-1587.
[52] 张立民,刘凯. 基于深度玻尔兹曼机的文本特征提取研究[J]. 微电子学与计算机,2015,32(2):142-147.
[53] 周盈盈,范磊. 基于改进词向量模型的深度学习文本主题分类[J]. 计算机科学与应用,2016,6(11):629-637.
[54] 李阳辉,谢明,易阳. 基于深度学习的社交网络平台细粒度情感分析[J]. 计算机应用研究,2017,34(3):743-747.
[55] 雷亚国,贾峰,周昕,等. 基于深度学习理论的机械装备大数据健康监测方法[J]. 机械工程学报,2015,51(21):49-56.
[56] 潘儒扬,李乡儒. 基于深度学习技术的恒星大气物理参数自动估计[J]. 天文学报,2016,57(4):379-388.
[57] 谭娟,王胜春. 基于深度学习的交通拥堵预测模型研究[J]. 计算机应用研究,2015,32(10):2951-2954.
[58] 潘志刚,刘三明,李莹,等. 基于深度学习网络的风电场功率短期预测研究[J]. 科技与创新,2015,43(19):4-6.
[59] 夏春江,王培良,张媛. 基于深度学习的木材含水率预测[J]. 杭州电子科技大学学报,2015,35(1):31-35.
[60] 姚俊杨,许继平,王小艺,等. 基于深度学习的湖库藻类水华预测研究[J]. 计算机与应用化学,2015,32(10):1265-1268.