

《信息安全测评理论与技术》专辑 前言

冯登国

由于信息安全问题直接影响到国家安全,世界各国都高度重视,并纷纷通过颁布标准、实行有效的测评认证制度等方式,对信息技术产品和信息系统实行严格的管理与控制.各国政府均投入巨资,由国家主导,针对不同的信息安全需求和技术领域研发相应的测评技术、方法和工具,以建立有效的信息安全测评认证体系,为保障本国的信息安全发挥重要作用.

信息安全测评(又称信息安全测试与评估)作为信息系统安全工程过程(ISSE)中的关键环节,在整个信息系统的生命周期中具有十分重要的作用,关系到信息系统安全建设的成败.信息安全测评的对象从传统的通信系统、操作系统、网络系统发展到涵盖技术和管理在内的完整的信息安全保障体系.

美国国家标准技术局(NIST)发布的信息系统安全自评估指南(SP800-26)是一种定性的风险评估方法,主要通过调查问卷对系统进行分析,并给出相应的管理控制措施、运行控制措施和技术控制措施.美国首席信息官委员会(CIO Council)联合美国审计总署(GAO)提出的联邦信息技术安全评估体系从五个层次来评估机构的安全状况,并帮助制定改善措施的优先次序,从而为各机构进行风险分析与评估提供指导.卡内基·梅隆大学开发的 OCTAVE 操作指南提供了对信息系统进行安全自评估的方法,它定义了一个资产驱动的、全面的、自定向的安全风险评估方法,适用于大型机构复杂信息系统的安全评估.

在信息安全测评技术和工具研发方面,目前的热点问题是如何将信息安全测评工程的指导模型、工作流程、评估方法、文档模板、测评工具和安全数据等方面进行规范化、自动化和定量化.典型的测评工具包括基于专家系统的评估工具(如 COBRA、@RISK、BDSS 等)和基于过程式算法的评估工具(如 CRAMM、RA 等).从量化程度来区分,包括定性评估工具(如 CONTROL-IT、Definitive Scenario、JANBER 等)和半定量评估工具(如 COBRA、@RISK、BDSS、The Buddy System、RiskCALC、CORA 等),目前还没有完全量化的信息安全测评工具.

我国的多家信息安全测评机构、高等院校及科研机构在信息安全测评模型、关键技术及平台工具的研发领域做了大量工作,并取得了一系列重要成果,研制了一批测评工具,有的已经相继投入到实际的测评工作中,包括密码算法与产品测试工具、操作系统安全性测试工具、信息安全产品测评工具、信息系统风险评估平台、系统交易处理性能测试系统、可信计算测试平台,等等.

我国政府各部门、重要行业的信息化建设工作,涉及到系统规划、产品选型、质量监督、运营维护等多个环节的安全性问题,迫切需要采用先进的信息安全测评方法、技术及配套工具,对信息产品和信息系统进行全面、可靠、可控的安全测评,从而为我国的经济建设和社会发展建立强有力的信息安全保障体系,因此,信息安全测评的自主化和产业化是必经之路.

信息技术发展迅速,信息安全测评方法、技术和工具的发展也具有鲜明的时效性.目前,信息安全测评的发展趋势是智能化、综合化和服务一体化.与传统风险评估注重于脆弱性探测和威胁分析不同,信息安全测评将逐渐融合静态脆弱性分析和动态安全态势评估,基于主动防御思想挖掘各个层面的安全漏洞,利用数学模型和智能化分析算法对信息系统的安全脆弱性进行量化评估,在此基础上通过安全态势指标的动态采集、归并、关联、融合及评估,提供信息系统动态运行状况和安全态势的可视化表述及发展趋势预测.另一方面,信息安全测评与信息安全服务(例如安全咨询、体系规划、安全管理、应急响应等)将逐渐融为一体,构成信息系统生命周期的闭环保障体系,利用信息系统前期安全服务的分析数据,实现信息系统风险状况及发展态势的动态评估,为后期安全服务的合

理开展提供基础性指导. 当前我国开展的等级保护工作必将引领我国信息安全测评方法与技术的发展.

信息安全测评理论与技术是构建国家信息安全测评认证体系的基础,也是指导信息技术产品和信息系统的安全性测评的科学依据.《计算机学报》特别推出信息安全测评理论与技术专辑,目标是总结信息安全测评领域的热点问题和现状,展现信息安全测评理论与关键技术的重大科技成果,开拓信息安全领域的新方向.

本专辑面向国内外征集到了一大批高质量的学术论文,在这里向这些投稿者表示衷心感谢.但专辑收集的论文数量有限,不得不忍痛割爱,当然在取舍过程中也可能有不妥的地方,敬请诸位投稿者原谅.经过初审、复审、终审等过程最后录用了 24 篇论文,这些论文反映了当前信息安全测评领域的研究热点和最新研究进展,代表了中国在这一领域当前的最前沿的研究水平.这里还要特别感谢审稿者和编辑部所付出的辛勤劳动.

下面将从密码算法、安全协议、可信计算平台、信任、系统安全、网络安全等测评理论与技术简要总结一下本专辑的主要贡献.

本专辑收录了 4 篇密码算法和安全协议测评方面的论文,主要贡献是:

陈华等的论文“一种关于分组密码的新的统计检测方法”提出一种有效实用的统计检测方法,该方法以分组长度为统计单位,将一个分组的某一字节取遍所有的值而其它字节固定不变,经过密码变换后将 256 个输出值进行异或,通过检测输出异或值每一位为 0 或 1 的概率是否为 $1/2$ 来判断分组密码是否随机,并可反映出分组密码抵抗积分攻击的能力.

邓高明等的论文“针对密码芯片的频域模板分析攻击”提出一种在密码芯片电磁辐射频域信号上进行模板分析的方法,通过对运行 RC4 密码算法的微控制器的攻击实验表明,在密码程序中插入随机时延使得时域模板分析失效的情况下,对频域信号的分析依然可以恢复 RC4 的原始密钥.

胡予濮等的论文“一种改进的对三轮 OAEP 明文填充方案”对明文填充方案三轮 OAEP 进行了分析,指出它设计上存在两个缺陷,即填充方案本身不具有自认证功能和概率加密函数所使用的随机串是任意选择的.基于此发现,说明了当解密机可以输出填充方案中的随机串时,三轮 OAEP 在适应性选择密文攻击下是不安全的,并给出了攻击实例.

田园等的论文“基于刚性与相似性概念的密码协议分析方法”提出 Dolev-Yao 刚性和 Dolev-Yao 相似性概念,针对 strand-图模型证明了 Canetti 的 UC-相似性概念与 Dolev-Yao 相似性概念之间接近充分必要程度的对偶关系,从而对融合 UC-理论/strand-图模型具体证明了其分析框架具有相容性和完备性,并建立了一种新的协议分析方法.

本专辑收录了 3 篇可信计算平台测评方面的论文,主要贡献是:

徐明迪等的论文“基于标记变迁系统的可信计算平台信任链测试”使用进程代数作为形式化工具描述信任链,对信任链的行为特征进行推导,从动态的角度建立了基于标记变迁系统的信任链测试模型,并从易测试性的角度约简出信任链基本测试集,提出信任链的规范实现与规范说明之间的一致性关系.

陈小峰的论文“可信平台模块的形式化分析和测试”在分析可信平台模块目前存在的一些问题的基础上,给出了可信平台模块的形式化规格说明,基于该规格说明给出了扩展有限状态机模型,并将该有限状态机模型应用于测试用例的自动生成,通过实验验证了形式化测试的有效性.

李昊等的论文“可信密码模块符合性测试方法研究”提出一种可信密码模块(TCM)符合性测试的形式化方法,采用基于扩展有限状态机(EFSM)模型与测试向量相结合的方式对 TCM 的标准进行形式化建模.通过测试结果分析以及与其他相关工作的对比,表明该方法能够有效地产生测试用例,并可提高 TCM 符合性测试的错误检测率.

本专辑收录了 3 篇信任测评方面的论文,主要贡献是:

李小勇等的论文“基于行为监控的自适应动态信任度测模型”将粗糙集理论和信息熵理论结合起来,应用于开放环境下动态构建基于行为数据监控与分析的信任关系度测(度量与预测)模型.实

验结果表明,与已有模型相比,新模型能够快速准确地实现开放分布式环境下实体的可信性判别,并具有良好的行为数据规模的扩展能力。

胡东辉等的论文“盲环境下的数字图像可信性评估模型研究”提出盲环境下数字图像可信性评估概念,将可信性评估模型分为可信性判断模型和可信性度量模型两种。提出和设计了基于马尔夫模型数字图像可信性历史度量模型和基于模糊层次分析法的数字图像可信性综合度量模型。通过实验验证了所提出的数字图像可信性综合度量模型的有效性。

张润莲等的论文“一种基于实体行为风险评估的信任模型”提出一种基于实体行为风险评估的信任模型,该模型通过对实体行为的风险评估和量化,给出了基于风险的实体信任计算方法。应用实例及测试结果表明,该方法通过实体行为风险评估,可更加客观地反映实体的信任变化,从而为系统对实体的后续行为控制提供可靠的决策支持。

本专辑收录了 6 篇系统安全测评方面的论文,主要贡献是:

程亮等的论文“基于 UML 和模型检测的安全模型验证方法”提出一种基于 UML 和模型检测器的安全模型验证方法。该方法采用 UML 将安全策略模型描述为状态机图和类图,然后利用转换工具将 UML 图转化为模型检测器的输入语言,最后由模型检测器来验证安全模型对于安全需求的满足性,并使用该方法验证了 DBLP 模型对机密性原则的违反。

张阳的论文“带敏感标签的 SELinux 安全策略信息流分析方法”针对 SELinux 操作系统中多安全策略的实现方式,在信息流分析方法的基础上引入了多级安全敏感标签,以自动机与线性时态逻辑为理论基础,提出了一种改进的信息流分析方法,对 SELinux 安全策略的完整性与机密性进行验证。

咸鹤群的论文“机密数据库泄漏源检测与量化评估方案”提出一种基于复合型数据库水印的检测方法与量化评估方案,设计了复合型数据库水印的添加与检测算法,实现了泄漏源检测与追查过程中对参与双方的公平保护,使用概率分析的方法实现了检测结果的可靠性量化评估。实验结果表明,该方案具有较高的实用价值。

吴新松等的论文“基于静态分析的强制访问控制框架的正确性验证”提出 MAC 框架的 MAC 标记完全初始化原则、MAC 标记完全销毁原则和访问完全授权原则。提出一个路径敏感的、基于用户自定义检查规则的静态分析方法。该方法通过基于规则的集成于编译器之中的检查工具来验证 FreeBSD MAC 框架的正确性。

钮俊等的论文“一种刻画功能和时间空间性能的统一验证模型 atsFPM”提出一种刻画功能、时间和空间性能的组合形式化验证模型 atsFPM。用基于正则式的路径范式表示信息系统行为路径上的功能属性,并给出 atsFPM 模型的语法和形式语义。用基于 Markov 回报模型的性能验证技术解决 atsFPM 模型的功能性能组合验证问题,给出模型验证算法。

王昌达等的论文“一种隐通道威胁审计的度量方法”通过引入威胁度和威胁率两个概念给出了一种新的威胁审计方法,该方法与已有的纯带宽标准兼容,可从多个不同的角度对隐通道的威胁程度进行度量。并在隐通道代数系统的支持下给出了审计中有关问题的计算方法,形成了一套隐通道威胁度量体系。

本专辑收录了 8 篇网络安全测评方面的论文,主要贡献是:

韦勇等的论文“基于日志审计与性能修正算法的网络安全态势评估模型”提出基于日志审计与性能修正算法的网络安全态势评估模型,利用日志审计评估节点理论安全威胁,并通过性能修正算法计算节点安全态势,再利用节点服务信息计算网络安全态势,同时采用多种预测模型对网络安全态势进行预测,绘制安全态势曲线图。

刘家红等的论文“ProSPer:一个支持 proactive 特性的通用型事件监控系统”基于时序关系并不能提高事件监控的预测能力的假设,设计了基于 top- k 复合事件检测模型的事件监控系统 PROSPer,可为网络安全监控等应用系统提供 proactive 特性的事件监控能力。

张红斌等的论文“内部威胁云模型感知算法”定义了主体、客体两个偏序结构和二者间的映射

关系,建立了分层映射内部威胁模型;利用此模型定义了表征系统内部威胁状态的内部威胁云模型,并设计了基于云模型感知算法实现了对系统内部威胁的评测感知.实验结果表明,此算法能够实时、有效的感知系统的内部安全威胁.

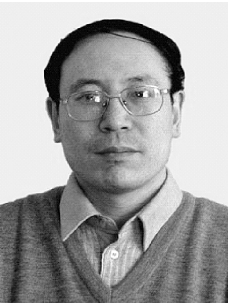
李伟明等的论文“一种优化的实时网络安全风险量化方法”将 IDS 告警和主机的漏洞、状态结合起来,定义攻击的威胁度来更好地体现攻击的风险,并对攻击进行分类,简化隐马尔科夫模型的输入.提出了利用遗传算法来自动求解隐马尔科夫模型中的矩阵,定义风险描述规则作为求解的优化目标,解决隐马尔科夫模型难以配置的问题.

付才等的论文“移动自组网中非完全信息节点风险评估”提出采用灰色系统理论描述通信节点非完全信息状态,根据灰类白化以及灰色聚类思想进行节点风险评估.分析与实际计算表明,该方法是一种适合移动自组网中非完全信息节点风险评估的有效方法.

姜伟等的论文“基于攻防博弈模型的网络安全测评和最优主动防御”提出了网络攻防策略分类及其成本量化模型、网络防御图模型、网络攻防博弈模型和基于上述模型的最优主动防御选取算法.通过一个典型的网络实例模拟和分析该模型及算法在网络安全评测和最优主动防御的应用.测试实验结果表明,提出的模型和方法是可行的、有效的.

朱建明等的论文“基于博弈论的信息安全技术评价模型”基于决策理论的入侵检测模型,对企业信息安全体系结构中的信息安全技术的价值进行评价.研究结果表明,入侵检测的正效益不是来自于检测率的提高,而是通过提高检测率增加了其威慑作用来体现的.

褚伟波等的论文“基于收发平衡判定的 TCP 流量回放方法”提出一种基于收发平衡和状态判定相结合的新的 TCP 流量回放方法.通过在发送 TCP 数据包前优先进行收发平衡判定将数据包发送出去,提出方法能够有效减少 TCP 流量在发送过程中的状态判定开销,提高回放性能.并对引入收发平衡机制前后的 TCP 流量回放方法的差异进行了分析比较.



冯登国,《计算机学报》副主编,信息安全国家重点实验室主任,国家信息化专家咨询委员会委员,国家“十五”863 计划信息安全技术主题专家组首席科学家,国家“十一五”863 计划信息技术领域专家组成员,长期从事信息安全理论与技术研究开发工作.