软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(8):2227−2228 [doi: 10.13328/j.cnki.jos.005769]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向自主安全可控的可信计算专题前言*

张焕国[1,2], 贾春福[3], 林璟锵[4]

[1](武汉大学 国家网络安全学院,湖北 武汉 430079)

[2](空天信息安全与可信计算教育部重点实验室(武汉大学),湖北 武汉 430079)

[3](南开大学 网络安全学院,天津 300071)

[4](信息安全国家重点实验室(中国科学院信息工程研究所),北京 100093)

通讯作者: 张焕国, E-mail: liss@whu.edu.cn

中文引用格式: 张焕国,贾春福,林璟锵.面向自主安全可控的可信计算专题前言.软件学报,2019,30(8):2227−2228. http://www.jos.org.cn/1000-9825/5769.htm

可信计算是一种旨在增强计算机系统可信性的综合性信息安全技术.其基本思想是,在计算机系统中建立一个信任根,从信任根开始到硬件平台,到操作系统,再到应用,一级度量认证一级,一级信任一级,把这种信任扩展到整个计算机系统,并采取防护措施,确保计算资源的完整性和行为的预期性,从而提高计算机系统的可信性.我国在可信计算领域起步不晚,创新很多,成果可喜.可信计算的综合性说明,它应当与其他信息安全技术相结合.例如,与密码技术、访问控制、硬件安全、软件安全、网络安全、内容安全等技术相结合.实践证明,这种结合会得到很好的效果.

为了加速发展我国信息安全领域的核心技术,《软件学报》与第 12 届中国可信计算与信息安全学术会议合作,推出了面向自主安全可控的可信计算专题.专题内容体现了可信计算与其他信息安全技术的结合.本专题共征收到 17 篇稿件.特约编辑邀请了相关领域专家参与审稿,每篇稿件至少由 2 位专家进行评审.通过专家评审的稿件,又经过编辑部的审核,确定出 10 篇稿件进入会议现场报告答辩.第 12 届中国可信计算与信息安全学术会议为此专设了一个“面向自主安全可控的可信计算”专场,在特邀编辑的主持下,每篇稿件都进行了现场报告和答辩.最终选定这 10 篇稿件入选本专题.

《恶意代码演化与溯源技术研究》综合论述了恶意代码演化与溯源领域的研究工作及其发展趋势.恶意代码是黑客攻击的主要武器,对攻击进行溯源是威慑和惩治攻击的重要手段.此方面研究是很多其他信息安全技术的基础,因此该文的内容是很有价值的.

《软件实时可信度量:一种无干扰行为可信性分析方法》提出了一种基于无干扰的软件实时可信度量方法,并进行了模拟实验.实验结果表明了该方法的有效性.可信度量是可信计算最重要的技术措施之一,而现有的可信度量仍有不足之处,需要改进提升.该文对此进行了充分讨论.

《基于 Duplication Authority 的 TPM2.0 密钥迁移协议》分析了《TPM-Rev-2.0-Part-1- Architecture-01.38》可信计算规范,并总结出使用该规范中的密钥复制接口来实施密钥迁移存在的 3 个问题.并针对这些问题,提出了一种新的密钥迁移新协议.实验结果表明,该协议不仅完全满足《TPM-Rev-2.0-Part-1- Architecture-01.38》规范,而且满足完整性、机密性和认证性.该文对 TPM2.0 的安全应用是有价值的.

《基于区块链的分布式可信网络连接架构》提出了一种基于区块链的分布式可信网络连接架构——B-TNC,并对 B-TNC 进行了正确性、安全性和效率分析.分析结果表明,B-TNC 能够实现面向分布式网络的可信网络连接,具有去中心化和较好的安全特性.可信网络连接(TNC)是一种重要的可信计算技术,可信网络连接架

* 收稿时间: 2019-03-01

构(TCA)是我国对 TNC 的一种改进方案.因此,该文的研究对于可信网络连接架构(TCA)的安全应用是有益的.

《Midori-64 算法的截断不可能差分分析》分析了 Midori-64 密码算法在截断不可能差分攻击下的安全性.文中给出了 11 轮 Midori-64 算法的不可能差分分析,恢复了 128 比特主密钥,其时间复杂度为 $2^{121.4}$,数据复杂度为 $2^{60.8}$,存储复杂度为 $2^{96.5}$.Midori 密码算法是一种设计用于资源受限环境的低功耗密码算法.分析 Midori 密码算法的安全性,对其应用和改进是很重要的.

《Piccolo 算法的相关密钥-不可能差分攻击》对 Piccolo 密码算法进行了安全性分析.分析结果表明,仅包含前向白化密钥的 15 轮 Piccolo-80 密码算法和 21 轮 Piccolo-128 密码算法在相关密钥-不可能差分攻击下是不安全的.Piccolo 密码算法也是一种设计用于资源受限环境的轻量级密码算法.分析 Piccolo 密码算法的安全性,对其应用和改进是很重要的.

《基于倒排索引的可验证混淆关键字密文检索方案》提出了一种基于倒排索引的可验证混淆关键字密文检索方案,并在真实数据集上进行了实验验证.实验结果表明,该方案在保证检索效率的同时,比现有的密文检索方案有效地提高了密文检索的安全性.基于云计算的数据中心是当前云计算最主要的应用之一.因此,该文的研究成果对于确保云计算中用户数据的安全是有价值的.

《无线传感器网络下多因素身份认证协议的内部人员攻击》指出了被长期忽略的内部攻击问题,对无线传感器网络环境下的两个代表性认证协议进行了安全性分析,指出其不安全问题,并提出了相应的解决方案.因此其研究是新颖而有意义的.

《基于 Laplace 机制的普适运动传感器侧信道防御方案》针对移动设备运动传感器侧信道攻击,提出了一种基于 Laplace 机制的传感器信号混淆防御方案.分析结果表明,该防御方案能够在保证 APP 正常运行的前提下,有效降低各种类型的运动传感器侧信道攻击成功率,从而具有良好的可用性.运动传感器广泛用于物联网和工业控制等系统中.确保这些系统的安全性是十分重要的.该文的研究对于物联网和工业控制等系统的安全可信具有参考意义.

《面向中文文本倾向性分类的对抗样本生成方法》为对抗样本攻击,提出了一种面向中文文本的对抗样本生成方法 WordHanding,并采用真实的数据集进行了实验验证.实验结果表明,该文方法是有效的.

最后,我们感谢《软件学报》和第 12 届中国可信计算与信息安全学术会议,感谢本专题的全体评审专家,感谢所有投稿作者!

张焕国(1945－),男,河北元氏人,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,可信计算,密码学.

贾春福(1967－),男,博士,教授,博士生导师,主要研究领域为系统与网络安全,软件安全,可信计算.

林璟锵(1978－),男,博士,教授,博士生导师,主要研究领域为密码应用安全.